

CompTIA.N10-009.v2026-10-20.q255

Exam Code:	N10-009
Exam Name:	CompTIA Network+ Certification Exam
Certification Provider:	CompTIA
Free Question Number:	255
Version:	v2026-10-20
# of views:	103
# of Questions views:	2766
https://www.freecram.net/torrent/CompTIA.N10-009.v2026-10-20.q255.html	

NEW QUESTION: 1

A network administrator is in the process of installing 35 PoE security cameras. After the administrator installed and tested the new cables, the administrator installed the cameras. However, a small number of the cameras do not work. Which of the following is the most reason?

- A. Incorrect wiring standard
- B. Power budget exceeded
- C. Signal attenuation
- D. Wrong voltage

Answer: (SHOW ANSWER)

When installing multiple Power over Ethernet (PoE) devices like security cameras, it is crucial to ensure that the total power requirement does not exceed the power budget of the PoE switch. Each PoE switch has a maximum power capacity, and exceeding this capacity can cause some devices to fail to receive power.

- * PoE Standards: PoE switches conform to standards such as IEEE 802.3af (PoE) and 802.3at (PoE+), each with specific power limits per port and total power capacity.
- * Power Calculation: Adding up the power requirements of all connected PoE devices can help determine if the total power budget of the switch is exceeded.
- * Symptoms: When the power budget is exceeded, some devices, typically those farthest from the switch or connected last, may not power up or function correctly.

Network References:

- * CompTIA Network+ N10-007 Official Certification Guide: Covers PoE standards and troubleshooting power issues.
- * Cisco Networking Academy: Discusses PoE technologies, power budgeting, and managing PoE devices.
- * Network+ Certification All-in-One Exam Guide: Provides information on PoE setup, including power budget considerations.

NEW QUESTION: 2

A CDN provider needs to implement a solution that delivers services to customers using IPv4, IPv6, or both to ensure interoperability. Which of the following technologies is the most appropriate for this requirement?

- A. Quality of service
- B. Automatic Private IP Addressing

C. Dual stack

D. Stateless Address Autoconfiguration

Answer: ([SHOW ANSWER](#))

Dual stack is the most appropriate technology because it allows a device, network, or service to support IPv4 and IPv6 at the same time. In a dual-stack environment, systems can communicate with IPv4-only clients, IPv6-only clients, and clients that support both protocol versions. This is especially important for a CDN provider because customers may connect from many different networks, and not all networks have fully migrated to IPv6.

The CompTIA Network+ N10-009 objectives include IPv4 and IPv6 addressing concepts, network services, and interoperability methods. Dual stack is a common transition strategy because it does not require immediate removal of IPv4. Instead, both protocol stacks operate together while networks gradually adopt IPv6.

Quality of service is used to prioritize traffic, not to provide IPv4 and IPv6 interoperability. Automatic Private IP Addressing assigns a 169.254.x.x address when DHCP fails and applies to IPv4 link-local addressing.

Stateless Address Autoconfiguration allows IPv6 hosts to create their own IPv6 addresses, but it does not provide IPv4 and IPv6 coexistence by itself. Therefore, dual stack is the correct answer.

NEW QUESTION: 3

Which of the following recovery strategies should a company implement to ensure data center services are quickly restored and accessible after a disaster occurs?

A. Backup and replication software

B. Active-passive approach

C. Cloud computing

D. Remote manual failover

Answer: ([SHOW ANSWER](#))

The correct answer is B. Active-passive approach. CompTIA Network+ N10-009 includes high availability and disaster recovery concepts such as failover, redundancy, and recovery strategies. An active-passive approach uses a primary production system, site, or service that actively handles traffic, while a secondary standby environment remains ready to take over if the primary environment fails. This design helps ensure data center services can be restored and made accessible quickly after a disaster because the standby environment is already planned and prepared for failover.

Backup and replication software is important for data protection, but backups alone do not guarantee that services will be quickly available.

Restoring systems from backups may require significant time. Cloud computing can support disaster recovery, but it is a broad deployment model rather than a specific recovery strategy. Remote manual failover can restore services, but manual failover usually takes longer and increases the chance of administrative delay or error.

Because the question emphasizes quickly restored and accessible services after a disaster, an active-passive approach is the most appropriate option. It provides a standby recovery environment designed to assume operations when the active data center service becomes unavailable.

NEW QUESTION: 4

A server administrator needs to add a record to the company's DNS server to verify ownership of a web domain. The administrator has the record's name and value. Which of the following record types should the administrator use to add the record to the DNS server?

A. TXT

B. A

C. PTR

D. CNAME

Answer: ([SHOW ANSWER](#))

To verify ownership of a domain, providers commonly require adding a TXT record to DNS containing a specific validation token (a name/value pair). A TXT (text) record is designed to store arbitrary text data associated with a domain or hostname, which makes it ideal for domain verification workflows used by certificate authorities, email security (SPF/DKIM/DMARC-related entries), and third-party services that need proof of administrative control over DNS. This fits Network+ DNS objectives that cover common record types and their practical purposes in real deployments.

An A record maps a hostname to an IPv4 address and is used for name-to-address resolution, not ownership verification. A PTR record provides reverse DNS mapping (IP address to hostname) and is stored in reverse lookup zones, not typically used for validating web domain ownership. A CNAME record creates an alias from one hostname to another canonical hostname; while sometimes used in service integrations, the classic "record name + token value" ownership verification is most directly and universally satisfied by a TXT record. Therefore, TXT is the correct choice given the requirement and the provided record name and value.

NEW QUESTION: 5

After a company installed a new IPS, the network is experiencing speed degradation. A network administrator is troubleshooting the issue and runs a speed test. The results from the different network locations are as follows:

Location	Speed Down	Speed Up
Wireless laptop	4.8 Mbps	47.1 Mbps
Wired desktop	5.2 Mbps	49.3 Mbps
Firewall	48.8 Mbps	49.5 Mbps

Which of the following is the most likely issue?

- A. Packet loss
- B. Bottlenecking
- C. Channel overlap
- D. Network congestion

Answer: ([SHOW ANSWER](#))

Bottlenecking occurs when a device in the network (such as an IPS) cannot process traffic efficiently, resulting in a dramatic drop in throughput. The significant difference between the firewall's speed (48.8 Mbps down) and the end-user devices' speeds (4.8 - 5.2 Mbps down) indicates a bottleneck caused by the IPS.

*Why not the other options?

*Packet loss (A) - Would typically cause connection timeouts, not just slow speeds.

*Channel overlap (C) - Affects only wireless networks, but the wired desktop is also experiencing slow speeds.

*Network congestion (D) - Would show fluctuations in both upload and download speeds, but upload speeds remain unaffected.

Reference:

CompTIA Network+ (N10-009) Official Guide - Chapter 13: Network Performance Optimization

NEW QUESTION: 6

A new backup system takes too long to copy files to the new SAN each night. A network administrator makes a simple change to the network and the devices to decrease backup times. Which of the following does the network administrator change?

- A. QoS
- B. SDN

- C. MTU
- D. VXLAN
- E. TTL

Answer: ([SHOW ANSWER](#))

Increasing the MTU (Maximum Transmission Unit) size allows larger frames to be transmitted, reducing overhead and improving throughput - especially for large file transfers like backups.

- A). QoS prioritizes traffic but doesn't reduce backup times directly.
- B). SDN is a network management model, not a parameter change.
- D). VXLAN encapsulates VLANs, not relevant to backup speeds.
- E). TTL is for packet lifetime, not throughput.

References (CompTIA Network+ N10-009):

Domain: Network Infrastructure - MTU, jumbo frames, performance tuning.

NEW QUESTION: 7

Which of the following is a cost-effective advantage of a split-tunnel VPN?

- A. Web traffic is filtered through a web filter.
- B. More bandwidth is required on the company's internet connection.
- C. Monitoring detects insecure machines on the company's network.
- D. Cloud-based traffic flows outside of the company's network.

Answer: ([SHOW ANSWER](#))

A split-tunnel VPN allows some traffic to be routed through the VPN while other traffic goes directly to the internet. This setup offers several advantages, with a primary one being cost-effectiveness due to cloud-based traffic not consuming company bandwidth.

* Bandwidth Utilization: Split-tunnel VPNs reduce the amount of traffic passing through the company's network, freeing up bandwidth for other uses.

* Performance: By allowing internet-bound traffic to bypass the VPN, it can reduce latency and improve the performance for users accessing cloud services directly.

* Cost Savings: Reduced load on the company's VPN infrastructure can lead to lower costs in terms of both hardware and bandwidth.

Network References:

* CompTIA Network+ N10-007 Official Certification Guide: Covers VPN types, including split-tunnel configurations and their advantages.

* Cisco Networking Academy: Discusses VPN technologies and the benefits of split-tunneling.

* Network+ Certification All-in-One Exam Guide: Provides detailed information on VPN setups, including the cost-effectiveness of split-tunnel VPNs.

By allowing cloud-based traffic to flow outside the company's network, a split-tunnel VPN optimizes resource usage and enhances the overall network performance without incurring extra costs for bandwidth.

NEW QUESTION: 8

Which of the following protocol ports should be used to securely transfer a file?

- A. 22
- B. 69
- C. 80
- D. 3389

Answer: ([SHOW ANSWER](#))

Port 22 is used for SFTP (Secure File Transfer Protocol) and SCP (Secure Copy Protocol), which encrypt file transfers using SSH (Secure Shell). This ensures data is transmitted securely over the network.

*Why not the other options?

*Port 69 (B) - TFTP (Trivial File Transfer Protocol): Transfers files but is not secure (no encryption).

*Port 80 (C) - HTTP: Used for web traffic, not for file transfer.

*Port 3389 (D) - RDP (Remote Desktop Protocol): Used for remote desktop access, not file transfer.

Reference:

CompTIA Network+ (N10-009) Official Guide - Chapter 5: Network Protocols and Ports

NEW QUESTION: 9

Which of the following impacts the availability of a web-based customer portal?

A. MAC flooding

B. ARP spoofing

C. DoS

D. Rogue devices

Answer: ([SHOW ANSWER](#))

A DoS (Denial of Service) attack directly targets availability, one of the core security goals (CIA triad) emphasized in Network+ (N10-009) security objectives. A web-based customer portal depends on reachable services (web servers, load balancers, DNS, upstream bandwidth). In a DoS, an attacker attempts to overwhelm the portal or its supporting infrastructure-consuming bandwidth, exhausting server resources, or saturating state tables-so legitimate users cannot connect or experience severe degradation. This is the most direct and common scenario where "availability" is impacted for a public web service.

MAC flooding aims to overflow a switch's CAM table and can lead to traffic being broadcast out ports, which is more commonly associated with enabling sniffing or disruption within a local switched network segment- not typically the primary attack described for a web portal's availability.

ARP spoofing is a local network man-in-the-middle/redirection technique affecting integrity/confidentiality and potentially availability for local hosts, but it is not the best match for a public portal availability impact. Rogue devices can introduce risk, but the option is broad and indirect; DoS is the clearest availability-focused threat.

NEW QUESTION: 10

A network technician was recently onboarded to a company. A manager has tasked the technician with documenting the network and has provided the technician With partial information from previous documentation.

Instructions:

Click on each switch to perform a network discovery by entering commands into the terminal. Fill in the missing information using drop-down menus provided.

Core Switch 1 Prompt



```
C:\> nmap
% Invalid input detected.
C:\> netdiscover
% Invalid input detected.
C:\> |
```

freecram.net

CompTIA®



Answer:

See the Explanation for detailed information on this simulation.

Explanation:

(Note: Ips will be change on each simulation task, so we have given example answer for the understanding) To perform a network discovery by entering commands into the terminal, you can use the following steps:

Click on each switch to open its terminal window.

Enter the command show ip interface brief to display the IP addresses and statuses of the switch interfaces.

Enter the command show vlan brief to display the VLAN configurations and assignments of the switch interfaces.

Enter the command show cdp neighbors to display the information about the neighboring devices that are connected to the switch.

Fill in the missing information in the diagram using the drop-down menus provided.

Here is an example of how to fill in the missing information for Core Switch 1:

The IP address of Core Switch 1 is 192.168.1.1.

The VLAN configuration of Core Switch 1 is VLAN 1: 192.168.1.0/24, VLAN 2: 192.168.2.0/24, VLAN 3: 192.168.3.0/24.

The neighboring devices of Core Switch 1 are Access Switch 1 and Access Switch 2.

The interfaces that connect Core Switch 1 to Access Switch 1 are GigabitEthernet0/1 and GigabitEthernet0/2.

The interfaces that connect Core Switch 1 to Access Switch 2 are GigabitEthernet0/3 and GigabitEthernet0/4.

You can use the same steps to fill in the missing information for Access Switch 1 and Access Switch 2.

NEW QUESTION: 11

Network administrators are using the Telnet protocol to administer network devices that are on the 192.168.1.0/24 subnet. Which of the following tools should the administrator use to best identify the devices?

- A. dig
- B. nmap
- C. tracer
- D. telnet

Answer: ([SHOW ANSWER](#))

nmap (Network Mapper) is the best tool in this scenario. It can scan the 192.168.1.0/24 subnet to discover live hosts, open ports (like Telnet on port 23), and device types. It's ideal for mapping and auditing the network.

- A). dig is a DNS lookup tool; not useful for identifying hosts on a subnet.
- C). tracer shows the path packets take to a destination, not for host discovery.
- D). telnet is the protocol being used, not a tool for scanning or identifying devices.

Reference:

CompTIA Network+ N10-009 Official Objectives: 5.1 - Given a scenario, use the appropriate network troubleshooting tools.

NEW QUESTION: 12

A company has been added to an unapproved list because of spam. The network administrator confirmed that a workstation was infected by malware. Which of the following processes did the administrator use to identify the root cause?

- A. Traffic analysis
- B. Availability monitoring
- C. Baseline metrics
- D. Network discovery

Answer: ([SHOW ANSWER](#))

Traffic analysis involves monitoring and inspecting network traffic flows to detect unusual patterns, such as a workstation sending large volumes of outbound SMTP (spam). This process enables identification of malware as the root cause.

- B). Availability monitoring checks uptime but doesn't diagnose spam traffic.
- C). Baseline metrics show normal usage but don't pinpoint infected hosts.
- D). Network discovery identifies devices, not malicious traffic flows.

References (CompTIA Network+ N10-009):

Domain: Network Security - Traffic analysis, malware detection, identifying compromised hosts.

NEW QUESTION: 13

Which of the following network devices converts wireless signals to electronic signals?

- A. Router
- B. Firewall
- C. Access point
- D. Load balancer

Answer: ([SHOW ANSWER](#))

* Role of an Access Point (AP):

- * **Wireless to Wired Conversion:**An access point (AP) is a device that allows wireless devices to connect to a wired network using Wi-Fi. It converts wireless signals (radio waves) into electronic signals that can be understood by wired network devices.
- * **Functionality:**
- * **Signal Conversion:**The AP receives wireless signals from devices such as laptops, smartphones, and tablets, converts them into electronic signals, and transmits them over the wired network.
- * **Connectivity:**APs provide a bridge between wireless and wired segments of the network, enabling seamless communication.
- * **Comparison with Other Devices:**
- * **Router:**Directs traffic between different networks and may include built-in AP functionality but is not primarily responsible for converting wireless to electronic signals.
- * **Firewall:**Protects the network by controlling incoming and outgoing traffic based on security rules, not involved in signal conversion.
- * **Load Balancer:**Distributes network or application traffic across multiple servers to ensure reliability and performance, not involved in signal conversion.
- * **Deployment:**
- * APs are commonly used in environments where wireless connectivity is needed, such as offices, homes, and public spaces. They enhance mobility and provide flexible network access.

References:

- * CompTIA Network+ study materials on wireless networking and access points.

NEW QUESTION: 14

A company has observed increased user traffic to gambling websites and wants to limit this behavior on work computers. Which of the following should the company most likely implement?

- A.** ACLs
- B.** Content filter
- C.** Port security
- D.** Screened subnet

Answer: (SHOW ANSWER)

A content filter blocks access to specific websites based on category, URL, or keywords. This is the best solution to restrict gambling websites.

Breakdown of Options:

- A). ACLs - Control network access, not specific web content.
- B). Content filter - # Correct answer. Used to block access to unwanted websites.
- C). Port security - Prevents unauthorized device connections, not web traffic filtering.
- D). Screened subnet - A DMZ isolates public-facing servers, not user restrictions.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 3.3: Given a scenario, implement network security measures.

NEW QUESTION: 15

A user reports network performance issues when accessing a specific server. Which of the following should be used to identify the cause of the issue in real time?

- A.** Port mirroring
- B.** Syslog reports
- C.** Baseline metrics

D. Packet capture

Answer: (SHOW ANSWER)

Packet capture is the best tool for identifying the cause of a network issue in real time. A packet capture allows a technician or administrator to inspect live network traffic between the client and server. It can reveal retransmissions, dropped connections, DNS problems, TCP handshake failures, latency symptoms, protocol errors, authentication issues, and application-level communication problems. This aligns with the CompTIA Network+ N10-009 troubleshooting objectives, which include using appropriate tools to diagnose network performance and connectivity issues. Port mirroring can be useful, but it is a switch feature that copies traffic from one port or VLAN to another monitoring port. It helps collect traffic, but by itself it does not analyze the packets. A packet capture tool is what actually records and inspects the traffic. Syslog reports are valuable for reviewing device logs, but they may not show real-time packet-level behavior between the user and the server. Baseline metrics are useful for comparison against normal performance, but they do not directly identify the immediate cause of a live issue. Therefore, packet capture is the most appropriate answer.

NEW QUESTION: 16

A network architect of a stock exchange broker is implementing a disaster recovery (DR), high-availability plan. Which of the following approaches would be the best fit?

- A. Warm site**
- B. Active-active**
- C. Full mesh**
- D. In-band**

Answer: (SHOW ANSWER)

The correct answer is Active-active because a stock exchange broker requires extremely high availability, minimal downtime, and near-zero data loss. According to CompTIA Network+ (N10-009) objectives under high availability and disaster recovery concepts, an active-active configuration involves multiple systems or sites operating simultaneously and sharing the workload. If one system fails, the other continues processing traffic without service interruption.

This model provides the lowest Recovery Time Objective (RTO) and Recovery Point Objective (RPO), which is critical in financial trading environments where even seconds of downtime can result in major financial loss. Active-active architectures also support load balancing, redundancy, and continuous synchronization between systems.

A warm site (Option A) contains preconfigured hardware but may require data restoration and configuration before becoming fully operational, resulting in some downtime. A full mesh (Option C) is a network topology design and does not specifically address disaster recovery at the service level. In-band (Option D) refers to management traffic sharing the production network and is unrelated to DR strategy.

Therefore, an active-active approach is the most suitable solution for mission-critical financial operations.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here: <https://www.edudump.com/exams/CompTIA/N10-009/premium/> (608 Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 17

Which of the following does a full-tunnel VPN provide?

- A. Lower bandwidth requirements
- B. The ability to reset local computer passwords
- C. Corporate Inspection of all networktraffic
- D. Access to blocked sites

Answer: (SHOW ANSWER)

A full-tunnel VPN routes all of a user's network traffic through the corporate network. This means that the organization can inspect all network traffic for security and compliance purposes, as all data is tunneled through the VPN, allowing for comprehensive monitoring and inspection.References:CompTIA Network+ study materials.

NEW QUESTION: 18

A user ' s home mesh wireless network is experiencing latency issues. A technician has:

- *Performed a speed test.
- *Rebooted the devices.
- *Performed a site survey.
- *Performed a wireless packet capture.

The technician reviews the following information:

SSID	MAC	RSS	Channel
Home	AAAAAA1111112	-83dBm	11
Home	AAAAAA1111113	-91dBm	11
Home	AAAAAA1111114	-70dBm	11

The technician notices in the packet capture that frames were retransmitted. Which of the following is the most likely cause of the user ' s network issue?

- A. The SSIDs should not be the same.
- B. The network has too much overlap.
- C. The devices are incompatible with the mesh network.
- D. The nodes are underpowered.

Answer: (SHOW ANSWER)

- *Too much overlap on the same channel (all devices on channel 11) causes interference, leading to retransmissions and high latency.
- *Same SSIDs (A) are expected in mesh networks.
- *Device compatibility (C) would show different symptoms.
- *Node power (D) affects coverage, not congestion.

Reference: CompTIA Network+ N10-009 Official Documentation - Wireless Troubleshooting & Signal Interference.

NEW QUESTION: 19

A security administrator is creating a new firewall object for a device with IP address 192.168.100.1/25.

However, the firewall software only uses dotted decimal notation in configuration fields. Which of the following is the correct subnet mask to use?

- A. 255.255.254.0
- B. 255.255.255.1

C. 255.255.255.128

D. 255.255.255.192

Answer: ([SHOW ANSWER](#))

A /25 subnet mask means 25 bits are reserved for the network portion, leaving 7 bits for host addresses. In dotted decimal, that is:

11111111.11111111.11111111.10000000

Decimal equivalent: 255.255.255.128

A). 255.255.254.0 corresponds to /23.

B). 255.255.255.1 is invalid as a subnet mask.

D). 255.255.255.192 corresponds to /26.

Thus, the correct subnet mask for a /25 network is 255.255.255.128.

References (CompTIA Network+ N10-009):

Domain: Networking Concepts - Subnetting, CIDR notation, dotted decimal.

NEW QUESTION: 20

Which of the following types of connectors allows the transmission of network data through a coaxial cable?

A. SC

B. MPO

C. BNC

D. RJ11

Answer: ([SHOW ANSWER](#))

The correct answer is BNC. A Bayonet Neill-Concelman connector, commonly called a BNC connector, is used with coaxial cable. Coaxial cabling has historically been used in Ethernet networks, cable broadband, CCTV systems, and radio frequency applications. BNC connectors use a twist-lock bayonet mechanism that provides a secure connection and helps maintain signal integrity over coaxial media.

The CompTIA Network+ N10-009 objectives include recognizing common cable types and connectors used in networking. SC and MPO are fiber-optic connectors, not coaxial connectors. SC connectors are commonly used for fiber connections and have a push-pull design. MPO connectors are multi-fiber push-on connectors often used in high-density fiber environments. RJ11 is commonly associated with telephone cabling and DSL connections, not coaxial Ethernet or RF-style network cabling. Since coaxial cable uses a central conductor, insulation, shielding, and an outer jacket, it requires connectors designed specifically for coaxial signaling.

Among the listed options, BNC is the connector type associated with transmitting network data over coaxial cable.

NEW QUESTION: 21

Which of the following, in addition to a password, can be asked of a user for MFA?

A. PIN

B. Favorite color

C. Hard token

D. Mother's maiden name

Answer: ([SHOW ANSWER](#))

Multi-factor authentication (MFA) requires two or more different categories of authentication factors:

Something you know (password, PIN)

Something you have (smart card, hardware token)

Something you are (biometric)

The only valid second factor here is a hard token (e.g., a key fob generating one-time codes).

A). PIN is still "something you know," the same category as a password.

B). Favorite color is a weak knowledge-based factor, not a true second factor.

D). Mother's maiden name is also "something you know" and insecure.

References (CompTIA Network+ N10-009):

Domain: Network Security - Authentication methods, MFA factor categories.

NEW QUESTION: 22

A few employees report issues with sessions disconnecting frequently, buffering repeatedly, and performing poorly. Given the following information:

- * Employees are in a multitenant office building.

- * The Wi-Fi uses 2.4GHz.

- * Wireless signals from users range between -50 to -65dBm.

- * WPA2 is used.

Which of the following is the most likely cause of the issues?

A. Channel overlap

B. Insufficient wireless coverage

C. AP antenna type

D. Outdated encryption usage

Answer: ([SHOW ANSWER](#))

The correct answer is A. Channel overlap. The signal strength numbers given, -50 to -65 dBm, are generally strong enough for normal client connectivity, so this does not point to weak coverage. The bigger clue is that the environment is a multitenant office building and the wireless network is using 2.4 GHz. That band is well known for congestion and overlapping channels, especially where many nearby businesses or tenants have their own access points.

In the 2.4 GHz range, there are only a few non-overlapping channels commonly used. When many APs operate close together on overlapping channels, clients can experience interference, retransmissions, poor throughput, buffering, and connection instability. Those symptoms fit the scenario very well.

The other options are less convincing. Insufficient wireless coverage does not line up with the reported signal levels. AP antenna type could matter in some designs, but there is nothing in the question pointing to a directional or placement issue. WPA2 is not the cause of the performance symptoms here; while it is older than WPA3, it does not normally create repeated buffering and disconnections in this way.

This is really a wireless interference question, and in a crowded 2.4 GHz building, channel overlap is the most likely reason.

NEW QUESTION: 23

A firewall administrator is mapping a server's internal IP address to an external IP address for public use.

Which of the following is the name of this function?

A. NAT

B. VIP

C. PAT

D. BGP

Answer: ([SHOW ANSWER](#))

Network Address Translation (NAT) is a process that allows a device, typically a firewall or router, to map private IP addresses to public IP addresses. This enables internal network devices to communicate over the internet using a single or a limited number of public IP addresses. Static NAT (One-to-One Mapping): Maps a single private IP address to a single public IP address, commonly used for servers that need to be accessible from the internet.

Dynamic NAT (Many-to-Many Mapping): Dynamically assigns a public IP from a pool to internal devices.

PAT (Port Address Translation): A type of NAT where multiple private IPs share a single public IP using different port numbers.

Incorrect Options:

B). VIP (Virtual IP Address): Used in load balancing and high-availability configurations, not for NAT.

C). PAT (Port Address Translation): A specific form of NAT, but the question refers to general NAT, making option A the best choice.

D). BGP (Border Gateway Protocol): A routing protocol used to exchange information between different networks, not related to NAT.

Reference:

CompTIA Network+ N10-009 Official Study Guide - Chapter on Network Address Translation (NAT)

NEW QUESTION: 24

A network engineer wants to implement a new IDS between the switch and a router connected to the LAN.

The engineer does not want to introduce any latency by placing the IDS in line with the gateway. The engineer does want to ensure that the IDS sees all packets without any loss. Which of the following is the best way for the engineer to implement the IDS?

A. Use a network tap.

B. Use Nmap software.

C. Use a protocol analyzer.

D. Use a port mirror.

Answer: ([SHOW ANSWER](#))

Reference: CompTIA Network+ Certification Exam Objectives - Network Security section.

NEW QUESTION: 25

A network administrator needs to divide 192.168.1.0/24 into two equal halves. Which of the following subnet masks should the administrator use?

A. 255.255.0.0

B. 255.255.254.0

C. 255.255.255.0

D. 255.255.255.128

Answer: ([SHOW ANSWER](#))

* Understanding Subnetting:

* Original Network: 192.168.1.0/24 has a subnet mask of 255.255.255.0, which allows for 256 IP addresses (including network and broadcast addresses).

* Objective: Divide this network into two equal subnets.

* Calculating Subnet Mask:

* New Subnet Mask: To divide 192.168.1.0/24 into two equal halves, we need to borrow one bit from the host portion of the address, changing the subnet mask to 255.255.255.128 (/25).

* Subnet Breakdown:

* First Subnet: 192.168.1.0/25 (192.168.1.0 - 192.168.1.127)

* Second Subnet: 192.168.1.128/25 (192.168.1.128 - 192.168.1.255)

* Verification:

* Each subnet now has 128 IP addresses (126 usable IP addresses, excluding the network and broadcast addresses).

* Comparison with Other Options:

* 255.255.0.0 (/16): Provides a much larger network, not dividing the original /24 network.

* 255.255.254.0 (/23): Also creates a larger subnet, encompassing more than the original /24 network.

* 255.255.255.0 (/24): Maintains the original subnet size, not dividing it.

References:

* CompTIA Network+ study materials on subnetting and IP addressing.

NEW QUESTION: 26

An IT department is considering implementing a SIEM solution to improve network security. The department wants to ensure that the SIEM system is able to ingest and analyze logs from all of the company's core devices. Which of the following is the most important consideration when selecting a SIEM solution?

A. Easy to manage

B. Cost

C. Compatibility

D. Features

Answer: (SHOW ANSWER)

The correct answer is C. Compatibility . A SIEM is only effective if it can successfully collect, normalize, and analyze data from the systems the organization relies on. Since the question specifically says the department wants the SIEM to ingest and analyze logs from all core devices , the most important factor is whether the SIEM is compatible with those devices, their log formats, and their supported methods of exporting events. This includes support for common logging methods such as syslog , SNMP traps, API integrations, agent- based collection, and vendor-specific event formats. Even a SIEM with excellent features will not deliver value if it cannot properly receive and interpret logs from firewalls, routers, switches, servers, and security appliances already in use.

The other choices matter, but they come after compatibility. Ease of management is helpful for daily operations. Cost is always a practical concern. Features can improve visibility and automation. However, none of those benefits matter much if the SIEM cannot integrate with the organization's actual environment.

For Network+ exam purposes, when log ingestion across many device types is the requirement, the top selection criterion is compatibility .

Without that foundation, correlation, alerting, and security analysis will be incomplete.

NEW QUESTION: 27

A network administrator receives complaints of intermittent network connectivity issues. The administrator investigates and finds that the network design contains potential loop scenarios. Which of the following should the administrator do?

A. Enable spanning tree

B. Configure port security

C. Change switchport speed limits

D. Enforce 802.1Q tagging

Answer: (SHOW ANSWER)

Spanning Tree Protocol (STP) is designed to detect and prevent Layer 2 loops by blocking redundant paths. If loops are possible in the design, enabling STP ensures network stability.

B). Port security controls endpoint MAC addresses, not loops.

C). Speed limits address bandwidth, not loop prevention.

D). 802.1Q tagging allows VLAN separation but does not resolve loops.

References (CompTIA Network+ N10-009):

Domain: Network Operations - Loop prevention, spanning tree, switch design.

NEW QUESTION: 28

Which of the following protocols is used to send networking status messages between clients and servers?

A. SSH

B. DHCP

C. NTP

D. SNMP

Answer: ([SHOW ANSWER](#))

The correct answer is SNMP (Simple Network Management Protocol) because it is specifically designed to collect and transmit network management and status information between managed devices and management systems. According to CompTIA Network+ (N10-009) objectives, SNMP is used for monitoring and managing network devices such as routers, switches, servers, and printers.

SNMP operates using a manager-agent model. The SNMP manager (such as a network monitoring server) communicates with SNMP agents installed on network devices. Agents send traps and inform messages, which are unsolicited status alerts indicating events such as device failures, high CPU usage, or link outages.

The manager can also poll agents to retrieve performance metrics and configuration details stored in the Management Information Base (MIB).

SSH (Option A) is used for secure remote administration. DHCP (Option B) dynamically assigns IP addresses. NTP (Option C) synchronizes time between devices. None of these protocols are designed for network status monitoring and alert messaging.

Therefore, SNMP is the correct protocol for sending networking status messages between devices and management systems.

Bottom of Form

NEW QUESTION: 29

A network administrator needs to monitor data from recently installed firewalls in multiple locations. Which of the following solutions would best meet the administrator's needs?

A. IDS

B. IPS

C. SIEM

D. SNMPv2

Answer: ([SHOW ANSWER](#))

SIEM (Security Information and Event Management) systems are used to aggregate and analyze log data from various sources, including firewalls, to detect potential security incidents and assist in regulatory compliance.

The document explains:

"SIEM solutions aggregate and analyze log and event data from multiple devices, including firewalls, across different locations. They help in real-time monitoring, incident response, and ensuring compliance with security policies."

NEW QUESTION: 30

Which of the following is a company most likely enacting if an accountant for the company can only see the financial department's shared folders?

- A. General Data Protection Regulation
- B. Least privilege network access
- C. Acceptable use policy
- D. End user license agreement

Answer: ([SHOW ANSWER](#))

Least privilege network access is a principle that restricts users' access rights to only what is necessary for them to perform their job functions. In this case, the accountant's access is limited to only the financial department's shared folders, ensuring that they cannot access other parts of the network unnecessarily. This reduces the risk of unauthorized access and potential data breaches. References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 31

Which of the following Layer 1 devices is responsible for the termination of fiber-optic connections on an SFP-capable switch?

- A. Transceiver
- B. Modem
- C. Ethernet NIC
- D. Repeater

Answer: A ([LEAVE A REPLY](#))

A transceiver is the correct answer because it is the Layer 1 (Physical Layer) component that physically terminates and converts fiber-optic signals on an SFP-capable switch. In CompTIA Network+ N10-009 objectives, transceivers-such as SFP, SFP+, QSFP, and QSFP+ modules-are explicitly identified as physical interface components that handle signal transmission and reception. These modules convert electrical signals from the switch into optical signals for fiber cabling (and vice versa), enabling communication over different media types and distances.

A modem is also a Layer 1 device, but its purpose is to modulate and demodulate signals for WAN technologies such as DSL or cable-it does not terminate fiber connections on switches. An Ethernet NIC provides network access for end devices like computers and servers and typically terminates copper Ethernet, not modular fiber interfaces on switches. A repeater regenerates and amplifies signals to extend cable distances but does not provide fiber termination or media conversion at a switch port.

According to Network+ standards, SFP transceivers are essential for flexible network design, allowing administrators to select appropriate fiber types (single-mode or multi-mode), wavelengths, and distances while remaining compliant with physical layer requirements.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here: <https://www.edudump.com/exams/CompTIA/N10-009/premium/> (608 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 32

A school purchases new equipment and needs to configure a routing protocol that minimizes configuration overhead and ensures fast convergence. Which of the following routing protocols is the most suitable choice?

- A. IS-IS
- B. OSPF
- C. RIPv2

D. BGP

Answer: ([SHOW ANSWER](#))

OSPF is the most suitable routing protocol because it provides fast convergence and is commonly used as an interior gateway protocol within organizations. OSPF is a link-state routing protocol that builds a topology database and calculates the best path using cost. When a network change occurs, OSPF can converge much faster than older distance-vector protocols such as RIPv2. It is also widely supported by enterprise routing equipment and is appropriate for campus, school, and organizational networks.

The CompTIA Network+ N10-009 objectives include routing technologies, dynamic routing protocols, administrative distance, convergence, and routing protocol selection. OSPF is often preferred in internal networks because it scales better than RIP and can be configured in a single area for relatively simple deployments, reducing configuration complexity.

IS-IS is also a link-state protocol and can converge quickly, but it is less commonly used in typical small or medium enterprise environments and may require more specialized knowledge. RIPv2 has simpler configuration but slower convergence and hop-count limitations. BGP is mainly used for external routing between autonomous systems and is not the best choice for an internal school network. Therefore, OSPF is correct.

NEW QUESTION: 33

Which of the following cloud service models most likely requires the greatest up-front expense by the customer when migrating a data center to the cloud?

- A.** Infrastructure as a service
- B.** Software as a service
- C.** Platform as a service
- D.** Network as a service

Answer: ([SHOW ANSWER](#))

Reference: CompTIA Network+ Certification Exam Objectives - Cloud Models section.

NEW QUESTION: 34

Which of the following would allow a network administrator to analyze attacks coming from the internet without affecting latency?

- A.** IPS
- B.** IDS
- C.** Load balancer
- D.** Firewall

Answer: ([SHOW ANSWER](#))

An Intrusion Detection System (IDS) monitors and analyzes traffic to detect suspicious activity but does not sit in the traffic path, meaning it doesn't affect latency. In contrast, an IPS is in-line and can introduce delay.

From Andrew Ramdayal's guide:

"IDS monitors and alerts on malicious activity but does not block traffic, making it suitable for environments where low latency is critical."

NEW QUESTION: 35

A company is implementing a new internal network in which all devices use IPv6 addresses. Which of the following routing protocols will be best for this setup?

- A.** EIGRP
- B.** OSPFv3
- C.** BGP4

D. iBGP

Answer: ([SHOW ANSWER](#))

For an internal network using IPv6, the best option listed is OSPFv3, which is the OSPF version designed to support IPv6 routing. In Network+ (N10-009) routing objectives, OSPF is a common interior gateway protocol (IGP) used within an organization (an autonomous system) to exchange routes dynamically and converge efficiently. OSPFv3 maintains the link-state approach of OSPF while adding IPv6 support, making it a strong fit for enterprise internal routing where multiple routers and subnets need dynamic path calculation and fast convergence.

BGP4 and iBGP are associated with BGP, primarily used for inter-domain routing on the internet and between large networks; while BGP can carry IPv6 (via MP-BGP), it is generally not the "best" default choice for a typical internal-only enterprise network unless there is a specific design reason. EIGRP can support IPv6 in some implementations, but Network+ typically emphasizes OSPF/OSPFv3 as the widely adopted, vendor-neutral IGP for IPv6 deployments. Given the options and the "best for this setup" wording, OSPFv3 is the most appropriate answer.

NEW QUESTION: 36

Which of the following does a router prioritize first in the route selection process?

- A. Prefix length**
- B. Metric**
- C. Administrative distance**
- D. Default route**

Answer: ([SHOW ANSWER](#))

In the router route selection process, the first priority is the longest prefix match, also known as prefix length.

According to CompTIA Network+ (N10-009) routing concepts, routers examine the destination IP address in the packet and compare it to entries in the routing table. When multiple routes exist, the router selects the route with the most specific match, meaning the route with the longest subnet mask (largest number of matching bits). For example, a /30 route is preferred over a /24, and a /24 is preferred over a /16 if all match the destination.

Only after the longest prefix match is determined do other factors come into play. Administrative distance (AD) is used to determine which routing source is more trustworthy when the same network is learned from different routing protocols (e.g., OSPF vs. RIP). Metric is then used within the same routing protocol to determine the best path (e.g., hop count, cost, bandwidth). A default route (0.0.0.0/0) is used only when no more specific match exists.

Therefore, prefix length is always evaluated first in route selection.

NEW QUESTION: 37

A junior network administrator is auditing the company network and notices incrementing input errors on a long-range microwave interface. Which of the following is the most likely reason for the errors?

- A. The parabolic signal is misaligned.**
- B. The omnidirectional signal is being jammed.**
- C. The omnidirectional signal is not strong enough to receive properly.**
- D. The parabolic signal uses improper routing protocols.**

Answer: ([SHOW ANSWER](#))

A misaligned parabolic antenna can cause a significant increase in input errors because the signal is not properly focused or directed towards the receiving antenna, resulting in poor reception and data corruption.

The document confirms:

"Misalignment of parabolic microwave antennas can lead to weak or incorrect signal reception, causing an increase in input errors and connectivity issues on the link."

NEW QUESTION: 38

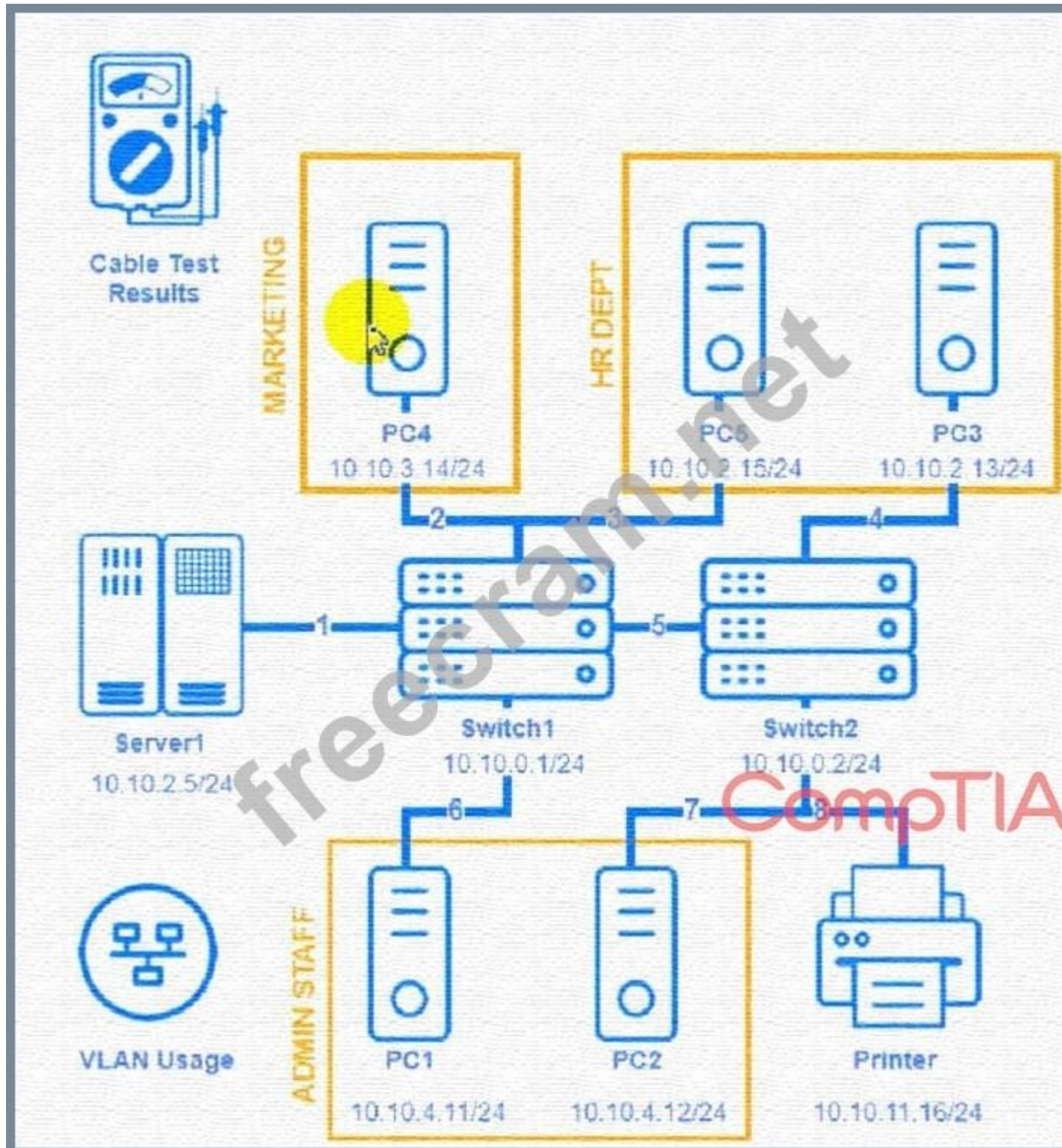
A network technician needs to resolve some issues with a customer 's SOHO network.

The customer reports that some of the devices are not connecting to the network, while others appear to work as intended.

INSTRUCTIONS

Troubleshoot all the network components and review the cable test results by Clicking on each device and cable.

Diagnose the appropriate component(s) by identifying any components with a problem and recommend a solution to correct each problem.





Cable Test Results:

Cable 1:

Cable 1	Cable 2	Cable 3	Cable 4	Cable 5	Cable 6	Cable 7	Cable 8
Length:	22M						
VLAN:	VLAN 2						
Speed:	1000 FDX						
Port:	GigabitEthernet0/1						

Cable 2:

Cable 3:

Cable 1	Cable 2	Cable 3	Cable 4	Cable 5	Cable 6	Cable 7	Cable 8
Length:	18M						
VLAN:	VLAN 2						
Speed:	1000 FDX						
Port:	GigabitEthernet0/3						

Cable 4:

Cable 1	Cable 2	Cable 3	Cable 4	Cable 5	Cable 6	Cable 7	Cable 8
Length: 20M				1	2	3	6
VLAN: VLAN 1				4	5	7	8
Speed: 1000 FDX				1	2	3	6
Port: GigabitEthernet0/2				4	5	7	8

Cable Test Results							
Cable 1	Cable 2	Cable 3	Cable 4	Cable 5	Cable 6	Cable 7	Cable 8
Length: 16M				1	2	3	6
VLAN: VLAN 1				4	5	7	8
Speed: 1000 FDX				1	2	3	6
Port: GigabitEthernet0/5				4	5	7	8

Cable Test Results

Cable 1

Cable 2

Cable 3

Cable 4

Cable 5

Cable 6

Cable 7

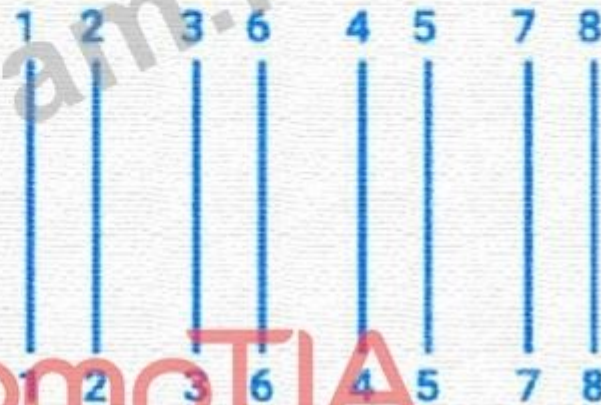
Cable 8

Length: 12M

VLAN: VLAN 1

Speed: 1000 FDX

Port: GigabitEthernet0/1



Printer

HP Network Configuration Page

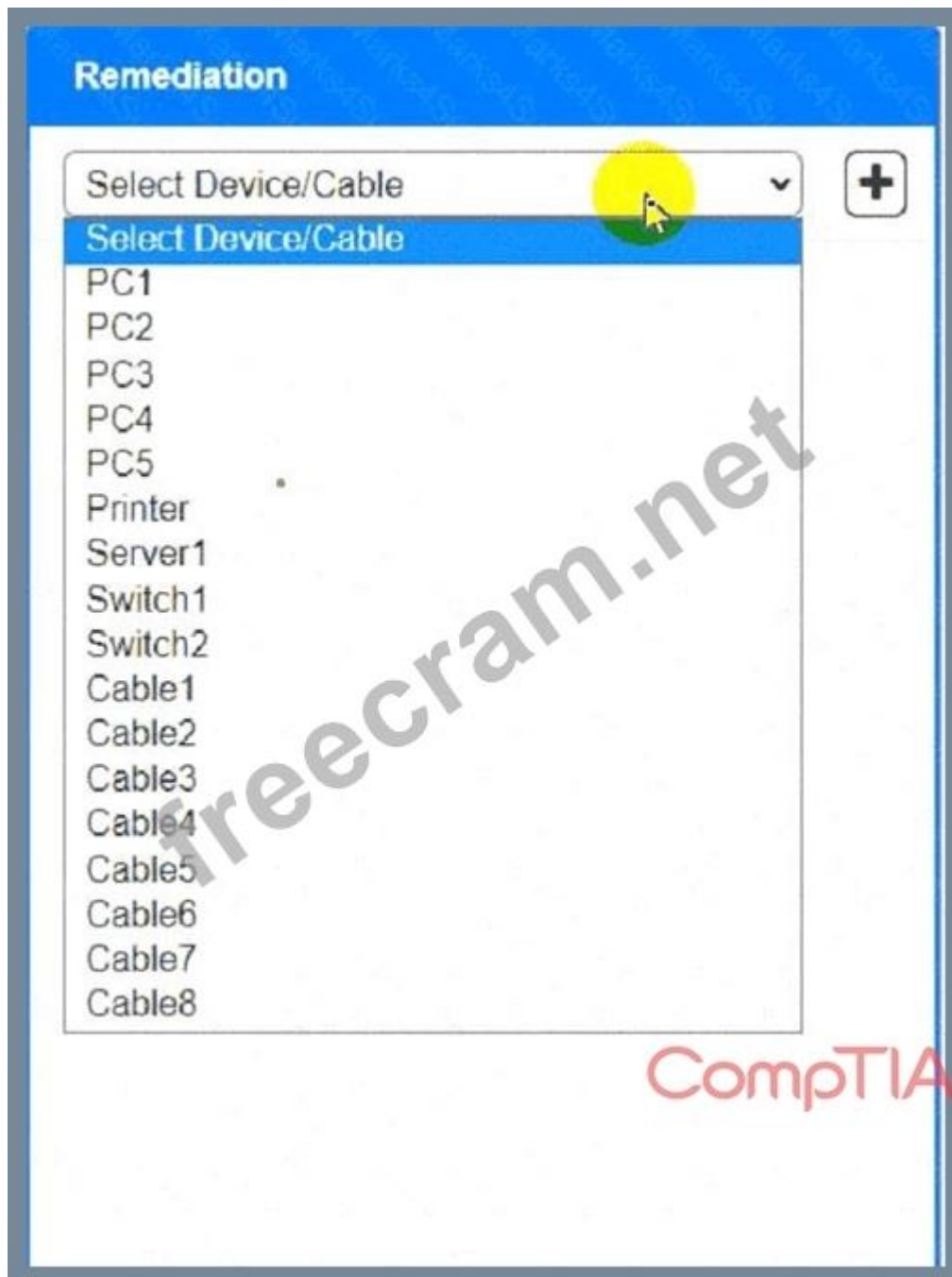
Model: HP Officejet Pro 8610

General Information

Network Status	Ready
Active Connection Type	Wired
URL(s) for Embedded Web Server	http://HP4D30EC , http://192.168.2.9
Firmware Revision	FDP1CN1347A
Hostname	HP4D30EC
Serial Number	CN3AO1KG42
Internet	Not Connected

802.3 Wired

Hardware Address (MAC)	9c b6 54 4d 30 ec
------------------------	-------------------



Answer:

See the Explanation for detailed information on this simulation.

Explanation:

(Note: Ips will be change on each simulation task, so we have given example answer for the understanding) To troubleshoot all the network components and review the cable test results, you can use the following steps:

Click on each device and cable to open its information window.

Review the information and identify any problems or errors that may affect the network connectivity or performance.

Diagnose the appropriate component(s) by identifying any components with a problem and recommend a solution to correct each problem.

Fill in the remediation form using the drop-down menus provided.

Here is an example of how to fill in the remediation form for PC1:

The component with a problem is PC1.

The problem is Incorrect IP address.

The solution is Change the IP address to 192.168.1.10.

You can use the same steps to fill in the remediation form for other components.

To enter commands in each device, you can use the following steps:

Click on the device to open its terminal window.

Enter the command `ipconfig /all` to display the IP configuration of the device, including its IP address, subnet mask, default gateway, and DNS servers.

Enter the command `ping < IP address >` to test the connectivity and reachability to another device on the network by sending and receiving echo packets. Replace `< IP address >` with the IP address of the destination device, such as 192.168.1.1 for Core Switch 1.

Enter the command `tracert < IP address >` to trace the route and measure the latency of packets from the device to another device on the network by sending and receiving packets with increasing TTL values.

Replace `< IP address >` with the IP address of the destination device, such as 192.168.1.1 for Core Switch 1.

Here is an example of how to enter commands in PC1:

Click on PC1 to open its terminal window.

Enter the command `ipconfig /all` to display the IP configuration of PC1. You should see that PC1 has an incorrect IP address of 192.168.2.10, which belongs to VLAN 2 instead of VLAN 1.

Enter the command `ping 192.168.1.1` to test the connectivity to Core Switch 1. You should see that PC1 is unable to ping Core Switch 1 because they are on different subnets.

Enter the command `tracert 192.168.1.1` to trace the route to Core Switch 1. You should see that PC1 is unable to reach Core Switch 1 because there is no route between them.

You can use the same steps to enter commands in other devices, such as PC3, PC4, PC5, and Server 1.

NEW QUESTION: 39

A user's desk has a workstation and an IP phone. The user is unable to browse the internet on the workstation, but the phone works. Which of the following configurations is required?

- A. Voice VLAN
- B. Native VLAN
- C. Data VLAN
- D. Trunk port

Answer: C (LEAVE A REPLY)

If the IP phone works but the workstation doesn't, it indicates that the Voice VLAN is functioning correctly, but the Data VLAN (C) is either misconfigured or missing. The workstation typically connects through the phone, which tags voice and data traffic separately using VLANs.

- * A. Voice VLAN is for the IP phone, which is already working.
- * B. Native VLAN is for untagged traffic on trunk ports, but doesn't control access directly.
- * D. Trunk port is more relevant to switch interconnections than individual workstation ports.

#Reference:

CompTIA Network+ N10-009 Official Objectives: 2.3 - Given a scenario, configure and verify VLANs.

NEW QUESTION: 40

A network administrator is configuring access points for installation in a dense environment where coverage is often overlapping. Which of the following channel widths should the administrator choose to help minimize interference in the 2.4GHz spectrum?

- A. 11MHz

- B. 20MHz
- C. 40MHz
- D. 80MHz
- E. 160MHz

Answer: ([SHOW ANSWER](#))

Reference: CompTIA Network+ Certification Exam Objectives - Wireless Networks section.

NEW QUESTION: 41

An organization has four departments that each need access to different resources that do not overlap. Which of the following should a technician configure in order to implement and assign an ACL?

- A. VLAN
- B. DHCP
- C. VPN
- D. STP

Answer: ([SHOW ANSWER](#))

VLANs (Virtual Local Area Networks) segment network traffic by department, allowing ACLs (Access Control Lists) to be applied based on VLAN membership, improving security and resource isolation.

Breakdown of Options:

- A). VLAN - Correct answer. VLANs enable logical network segmentation, allowing ACLs per department.
- B). DHCP - Assigns IP addresses but does not control access.
- C). VPN - Provides remote access, not segmentation within a network.
- D). STP - Prevents switching loops, not related to ACL implementation.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 1.3: Explain VLANs and network segmentation.

IEEE 802.1Q: VLAN tagging standard

NEW QUESTION: 42

Which of the following is a documented set of requirements, such as quality, availability, and responsibilities delivered by a vendor?

- A. MOU
- B. EOL
- C. EOS
- D. SLA

Answer: ([SHOW ANSWER](#))

The correct answer is SLA (Service Level Agreement) because it is a formal, documented contract between a service provider and a customer that defines expected service standards. According to CompTIA Network+ (N10-009) objectives under network operations and service management concepts, an SLA outlines measurable performance metrics such as uptime percentage, response time, throughput, support availability, escalation procedures, and responsibilities of both parties.

An SLA ensures accountability and establishes clear expectations for service delivery. For example, a vendor may guarantee 99.99% uptime, define maximum resolution times for incidents, and specify penalties or credits if performance targets are not met. SLAs are critical in cloud services, ISP agreements, managed services, and enterprise vendor contracts.

An MOU (Memorandum of Understanding) is a non-binding agreement outlining general terms between parties but does not define enforceable service metrics. EOL (End of Life) refers to when a product is no longer sold or supported. EOS (End of Support) indicates when a vendor stops providing updates or assistance for a product.

Therefore, an SLA is the correct document that defines vendor-delivered service requirements.

Top of Form

NEW QUESTION: 43

A network administrator notices uncommon communication between VMs on ephemeral ports on the same subnet. The administrator is concerned about that traffic moving laterally within the network. Which of the following describes the type of traffic flow the administrator is analyzing?

- A.** East-west
- B.** Point-to-point
- C.** Horizontal-scaling
- D.** Hub-and-spoke

Answer: ([SHOW ANSWER](#))

When traffic moves laterally between VMs within the same network or subnet, it is known as east-west traffic. This contrasts with north-south traffic, which refers to communication between internal and external networks.

Breakdown of Options:

- A). East-west - Correct answer. This refers to traffic between internal servers or VMs, which is a common security concern.
- B). Point-to-point - Point-to-point describes a direct connection between two devices, but does not specifically define lateral movement.
- C). Horizontal-scaling - This refers to adding more instances or nodes in cloud computing, unrelated to traffic flow.
- D). Hub-and-spoke - This network topology describes a centralized design, not lateral traffic.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 1.4: Analyze traffic patterns and behavior.

NIST SP 800-207: Zero Trust Architecture (ZTA) - East-West traffic monitoring

NEW QUESTION: 44

Due to concerns around single points of failure, a company decided to add an additional WAN to the network.

The company added a second MPLS vendor to the current MPLS WAN and deployed an additional WAN router at each site. Both MPLS providers use OSPF on the WAN network, and EIGRP is run internally. The first site to go live with the new WAN is successful, but when the second site is activated, significant network issues occur. Which of the following is the most likely cause for the WAN instability?

- A.** A changed CDP neighbor
- B.** Asymmetrical routing
- C.** A switching loop
- D.** An incorrect IP address

Answer: ([SHOW ANSWER](#))

Asymmetrical routing occurs when packets take different paths to and from the destination, leading to instability in network communication. The use of two different MPLS providers with OSPF can lead to this type of routing issue, especially if the paths aren't carefully configured and managed. This can cause unexpected routing behaviors and instability in a dual-WAN setup. (Reference: CompTIA Network+ Study Guide, Chapter on Network Routing)

NEW QUESTION: 45

A systems administrator is configuring a new device to be added to the network. The administrator is planning to perform device hardening prior to connecting the device. Which of the following should the administrator do first?

- A. Update the network ACLs.
- B. Place the device in a screened subnet.
- C. Enable content filtering.
- D. Change the default admin passwords.

Answer: (SHOW ANSWER)

Changing default admin passwords is a fundamental first step in device hardening to prevent unauthorized access.

NEW QUESTION: 46

A wireless technician wants to implement a technology that will allow user devices to automatically navigate to the best available frequency standard. Which of the following technologies should the technician use?

- A. Band steering
- B. Wireless LAN controller
- C. Directional antenna
- D. Autonomous access point

Answer: (SHOW ANSWER)

Band Steering: This technology enables wireless devices to connect to the most optimal frequency band (2.4 GHz or 5 GHz) by encouraging capable devices to switch to the less congested 5 GHz band. This improves overall network performance and prevents overcrowding on the 2.4 GHz band.

Wireless LAN controller (B): This manages multiple access points in a network but does not handle frequency optimization.

Directional antenna (C): This focuses the signal in a specific direction but does not affect frequency selection.

Autonomous access point (D): This operates independently but lacks advanced features like band steering.

Reference: CompTIA Network+ Official Study Guide, Domain 1.6 (Wireless Standards and Technologies).

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here: <https://www.edudump.com/exams/CompTIA/N10-009/premium/> (608 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 47

A network administrator receives a message that a duplicate IP address is on the network. Which of the following commands should the administrator use to locate the node?

- A. arp
- B. ping
- C. ipconfig
- D. nslookup

Answer: (SHOW ANSWER)

The arp command is the best choice for locating a node with a duplicate IP address. Address Resolution Protocol maps IPv4 addresses to MAC addresses on the local network. When a duplicate IP address warning appears, an administrator can use the ARP table to identify the MAC address associated with the conflicting IP address. After the MAC address is known, the administrator can check the switch MAC address table to determine which switch port the device is connected to.

This matches the CompTIA Network+ N10-009 troubleshooting objectives, which include using command-line tools to diagnose network issues. The arp -a command is especially useful when troubleshooting local IPv4 addressing conflicts because it displays known IP-to-MAC mappings. The ping command can test reachability, but it does not reliably identify the physical node causing the conflict. The ipconfig command displays or refreshes IP settings on the local Windows host, but it does not locate another device on the network. The nslookup command troubleshoots DNS name resolution, not duplicate IP addresses. Therefore, arp is the best command for this situation.

NEW QUESTION: 48

Which of the following should be used to obtain remote access to a network appliance that has failed to start up properly?

- A.** Crash cart
- B.** Jump box
- C.** Secure Shell (SSH)
- D.** Out-of-band management

Answer: ([SHOW ANSWER](#))

If a network appliance fails to start, standard remote access methods like SSH won't work. Instead, Out-of-Band (OOB) management provides a dedicated access path (e.g., a console port or iDRAC/iLO), allowing administrators to troubleshoot devices even when the network is down.

Breakdown of Options:

- A). Crash cart - A physical monitor/keyboard setup, not a remote solution.
- B). Jump box - A hardened system used for secure remote access but requires the device to be operational.
- C). Secure Shell (SSH) - Requires the device to be fully booted and network-connected.
- D). Out-of-band management - # Correct answer. Provides independent access for troubleshooting failed network devices.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 4.3: Explain network device management concepts.

NEW QUESTION: 49

A network technician is troubleshooting a web application's poor performance. The office has two internet links that share the traffic load. Which of the following tools should the technician use to determine which link is being used for the web application?

- A.** netstat
- B.** nslookup
- C.** ping
- D.** tracer

Answer: ([SHOW ANSWER](#))

* Understanding Tracer:

* Traceroute Tool:tracert(Windows) ortraceroute(Linux) is a network diagnostic tool used to trace the path that packets take from a source to a destination. It lists all the intermediate routers the packets traverse.

* Determining Traffic Path:

* Path Identification:By runningtracertto the web application's destination IP address, the technician can identify which route the traffic is taking and thereby determine which internet link is being used.

* Load Balancing Insight: If the office uses load balancing for its internet links, `tracert` can help verify which link is currently handling the traffic for the web application.

* Comparison with Other Tools:

* `netstat`: Displays network connections, routing tables, interface statistics, and more, but does not trace the path of packets.

* `nslookup`: Used for querying DNS to obtain domain name or IP address mapping, not for tracing packet routes.

* `ping`: Tests connectivity and measures round-trip time but does not provide path information.

* Implementation:

* Open a command prompt or terminal.

* Execute `tracert [destination IP]` to trace the route.

* Analyze the output to determine the path and the link being used.

References:

* CompTIA Network+ study materials on network troubleshooting and diagnostic tools.

NEW QUESTION: 50

A technician needs to quickly set up a network with five wireless devices. Which of the following network types should the technician configure to accomplish this task?

A. Ad hoc

B. Spine and leaf

C. Point to point

D. Mesh

Answer: (SHOW ANSWER)

The correct answer is Ad hoc because it allows wireless devices to communicate directly with one another without requiring a centralized access point or additional infrastructure. According to CompTIA Network+ (N10-009) objectives under wireless networking concepts, an ad hoc network (also known as an Independent Basic Service Set, or IBSS) enables peer-to-peer wireless communication.

This type of network is ideal for temporary or quick setups where only a small number of devices need to connect. In an ad hoc configuration, each device connects directly to others, making it simple and fast to deploy without requiring switches, routers, or wireless access points.

Spine and leaf (Option B) is a data center architecture designed for high scalability and redundancy, not small wireless setups. Point-to-point (Option C) refers to a direct connection between two devices only, which would not support five devices efficiently. Mesh (Option D) allows multiple nodes to interconnect and provide redundancy, but it is more complex and typically requires compatible infrastructure devices.

Therefore, for a quick setup with five wireless devices, an ad hoc network is the most appropriate choice.

NEW QUESTION: 51

Which of the following source control features allows an administrator to test a new configuration without changing the primary configuration?

A. Central repository

B. Conflict identification

C. Branching

D. Version control

Answer: (SHOW ANSWER)

Branching allows developers and administrators to create an isolated copy of the main configuration so they can test changes independently. This avoids impacting the primary environment and allows for safer testing and development.

Reference: Section 3.5 - Network Access and Management Methods - "Source Control: Branching"

NEW QUESTION: 52

A company ' s Chief Information Security Officer requires that servers and firewalls have accurate time stamps when creating log files so that security analysts can correlate events during incident investigations.

Which of the following should be implemented?

- A. Syslog server
- B. SMTP
- C. NTP
- D. SNMP

Answer: ([**SHOW ANSWER**](#)**)**

The correct solution is NTP (Network Time Protocol). Accurate timestamps across servers, firewalls, and network devices are critical for correlating logs during incident response. NTP synchronizes device clocks to a trusted time source, ensuring consistency across the network.

- A). Syslog centralizes logs but does not synchronize time.
- B). SMTP is email transfer, unrelated to time.
- D). SNMP monitors devices but does not correct time discrepancies.

By implementing NTP, analysts can ensure that logs from different devices are time-aligned, which is essential for reconstructing attack timelines and detecting anomalies.

References (CompTIA Network+ N10-009):

Domain: Network Operations - Time synchronization, NTP, log correlation.

NEW QUESTION: 53

Which of the following steps of the troubleshooting methodology should a technician take to confirm a theory?

- A. Duplicate the problem.
- B. Identify the symptoms.
- C. Gather information.
- D. Determine any changes.

Answer: ([**SHOW ANSWER**](#)**)**

To confirm a theory in the troubleshooting process, the technician should duplicate (replicate) the problem under controlled conditions. In the Network+ (N10-009) methodology, confirming a theory means validating that the suspected cause actually produces the observed symptoms. Replicating the issue helps ensure the technician is not chasing a coincidence, and it allows changes to be tested safely (for example, reproducing the issue with a specific user account, endpoint, cable, port, SSID, or configuration). If the problem can be duplicated, the technician can then try targeted actions to see whether the symptoms change in predictable ways-strengthening or disproving the hypothesis.

The other choices occur earlier as part of forming the theory. Identify the symptoms is an initial step to define the problem clearly. Gather information is part of the discovery phase-collect logs, error messages, topology details, and user observations. Determine any changes is also an early step used to correlate recent modifications (patches, new devices, config changes) with the onset of the issue. Those steps help create a theory; duplication helps confirm it before implementing a full fix.

NEW QUESTION: 54

A network administrator wants an automatic alert to be sent when a switch ' s link status changes, administered through SNMP. Which of the following SNMP technologies will allow for this alert?

- A. Trap

- B. Object identifier
- C. String
- D. MIB

Answer: A ([LEAVE A REPLY](#))

The right answer is A. Trap . In SNMP, a trap is an unsolicited notification sent from a managed device to the management system when a significant event happens. A switch detecting that an interface has gone up or down is a textbook example of the kind of event that can trigger this kind of message.

That is different from normal SNMP polling, where the monitoring server asks the device for status information on a schedule. With a trap, the device does not wait to be asked. It sends the alert immediately, which makes it useful for link failures, threshold violations, and other time-sensitive conditions.

The other choices are related to SNMP, but not in the same way. An object identifier (OID) points to a specific managed value. A string is commonly associated with SNMP community information in older versions. A MIB is the structured database of manageable objects. None of those are the actual alerting mechanism.

Because the question asks for an automatic alert when link status changes, the feature being described is clearly an SNMP trap .

NEW QUESTION: 55

A technician is implementing a new SD-WAN device with a default configuration. The technician receives a URL via email and connects the new device to the internet to complete the installation. Which of the following is this an example of?

- A. SASE device installation
- B. Zero-touch provisioning
- C. Infrastructure as code
- D. Configuration management

Answer: ([SHOW ANSWER](#))

This process describes Zero-touch provisioning (ZTP), where a device automatically pulls its configuration from a cloud controller or URL once connected to the internet. It's common in SD-WAN and modern network appliances.

- A). SASE (Secure Access Service Edge) refers to cloud-delivered network security, not a provisioning method.
- C). Infrastructure as code automates infrastructure deployment using code, but this scenario specifically fits ZTP.
- D). Configuration management tracks and maintains system configurations but doesn't describe the installation process.

Reference:

CompTIA Network+ N10-009 Official Objectives: 4.3 - Explain remote access methods and automation.

NEW QUESTION: 56

Which of the following is a type of NAC that uses a set of policies to allow or deny access to the network based on the user's identity?

- A. Standard ACL
- B. MAC filtering
- C. 802.1X
- D. SSO

Answer: ([SHOW ANSWER](#))

802.1X is a port-based Network Access Control (NAC) method that enforces authentication before allowing access to the network. It uses a RADIUS server for identity verification and policy enforcement, ensuring only authorized users/devices gain access.

- A). Standard ACL filters traffic by IP, not identity.

B). MAC filtering controls devices by hardware address but can be spoofed.

D). SSO (Single Sign-On) provides user convenience across services, not network-level access control.

References (CompTIA Network+ N10-009):

Domain: Network Security - NAC, 802.1X authentication, identity-based access.

NEW QUESTION: 57

Which of the following provides two switches with the most uptime if a power outage occurs?

A. Plugging both switches into the same PDU

B. Plugging each switch into a different circuit

C. Plugging each switch into a different PDU

D. Plugging each switch into a different UPS

Answer: ([SHOW ANSWER](#))

Plugging each switch into a different UPS provides the most uptime during a power outage. A UPS, or uninterruptible power supply, provides temporary battery power when utility power fails. Using separate UPS units also improves redundancy because a failure of one UPS does not necessarily affect both switches. This design helps maintain network availability and supports fault tolerance during electrical outages.

The CompTIA Network+ N10-009 objectives include network availability, redundancy, power management, UPS usage, and environmental considerations. Network switches are critical infrastructure devices, and loss of switch power can disconnect users, servers, wireless access points, VoIP phones, and other dependent systems. A UPS gives administrators time to maintain operations during short outages or shut systems down gracefully during longer outages.

Plugging both switches into the same PDU creates a single point of failure. Plugging each switch into a different circuit improves electrical redundancy, but it does not provide backup power if both circuits lose utility power. Plugging each switch into a different PDU can help with power distribution, but a PDU alone does not provide battery backup unless connected to a UPS. Therefore, different UPS units provide the best uptime.

NEW QUESTION: 58

As part of a recovery strategy, a network administrator needs to make sure no more than eight hours of data loss occurs. Which of the following DR metrics describes this requirement?

A. RPO

B. MTTR

C. RTO

D. MTBF

Answer: A ([LEAVE A REPLY](#))

Recovery Point Objective (RPO) defines the maximum acceptable amount of data loss measured in time. If leadership states "no more than eight hours of data loss," they are describing how far back the organization is willing to roll data after an outage or disaster-meaning backups, replication, snapshots, or journaling must ensure recoverable data is no older than eight hours. In Network+ terms, this is a core availability and resiliency planning concept: you choose an RPO based on business impact, then implement backup frequency

/replication strategy to meet it. By contrast, Recovery Time Objective (RTO) is about how quickly services must be restored (downtime duration), not how much data can be lost. MTTR (Mean Time to Repair/Recover) is an operational reliability metric describing typical time to restore a system, and MTBF (Mean Time Between Failures) indicates expected time between failures-neither directly states acceptable data loss.

Therefore, the metric matching "eight hours of data loss" is RPO.

NEW QUESTION: 59

A network technician is attempting to harden a commercial switch that was recently purchased. Which of the following hardening techniques best mitigates the use of publicly available information?

- A. Changing the default password
- B. Blocking inbound SSH connections
- C. Removing the gateway from the network configuration
- D. Restricting physical access to the switch

Answer: ([SHOW ANSWER](#))

Changing the default password is a fundamental step in device hardening, as default credentials are widely known and published online, posing a significant security risk if not updated. The document notes:

"Default passwords are often known by attackers and published on the internet. Changing them to unique, strong passwords is a critical first step in securing network devices against unauthorized access."

NEW QUESTION: 60

A network administrator is configuring a network for a new site that will have 150 users. Within the next year, the site is expected to grow by ten users. Each user will have two IP addresses (one for a computer and one for a phone). Which of the following classful IPv4 address ranges will be best-suited for the network?

- A. Class D
- B. Class B
- C. Class A
- D. Class C

Answer: ([SHOW ANSWER](#))

*The total number of devices = $(150 + 10)$ users $\times$ 2 IPs per user = 320 devices

*Class C (D) supports a maximum of 254 hosts ($2^8 - 2$), which is too small.

*Class B (B) supports 65,534 hosts ($2^{16} - 2$), making it the best choice.

*Why not the other options?

*Class A (C): Supports millions of addresses, which is overkill for 320 devices.

*Class D (A): Used for multicast, not for device addressing.

Reference:

CompTIA Network+ (N10-009) Official Guide - Chapter 7: IP Addressing and Subnetting

NEW QUESTION: 61

A small business is choosing between static and dynamic routing for its network. Which of the following is the best reason to use dynamic routing in a growing network?

- A. Easier to configure compared to using manually entered routes
- B. Does not require additional network security controls
- C. Features enhanced network monitoring and visibility
- D. Includes automatic changes and updates in network topology

Answer: ([SHOW ANSWER](#))

Dynamic routing is most beneficial in a growing/changing network because it can automatically learn, adapt, and update routes as the topology changes. In Network+ (N10-009) routing objectives, dynamic routing protocols exchange routing information between routers and recalculate

paths when links go down, new networks are added, or metrics change. This reduces the operational burden and the risk of human error that increases as the environment scales. With dynamic routing, adding a new subnet or branch often requires far fewer manual updates because routers propagate new route information automatically, and convergence mechanisms help restore connectivity after failures.

Option A can be partly true in large environments, but the core "best reason" emphasized for dynamic routing is the automatic adaptation to topology changes. Option B is incorrect-dynamic routing may introduce additional security considerations (route filtering, authentication, neighbor control). Option C is not a defining advantage; monitoring visibility depends on tools/telemetry rather than routing type. Therefore, the strongest and most correct reason is automatic changes and updates in network topology.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here: <https://www.edudump.com/exams/CompTIA/N10-009/premium/> (**608** Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 62

Users report that they cannot print to a specific IPv4-enabled printer after an extended power outage. Which of the following should a technician configure?

- A. DoH
- B. SLAAC
- C. APIPA
- D. DHCP reservation

Answer: ([SHOW ANSWER](#))

The correct answer is D. DHCP reservation. In a network environment, printers are typically configured to use a consistent IP address so that client devices can reliably locate them. After a power outage, network devices such as printers may reboot and request a new IP address from the DHCP server. If the printer was previously assigned a dynamic IP address, it may now receive a different address, causing users' systems to lose connectivity because they are still trying to print to the old IP.

A DHCP reservation ensures that a specific device (identified by its MAC address) always receives the same IP address from the DHCP server. This combines the convenience of DHCP with the stability of static addressing, which is ideal for shared resources like printers.

The other options are incorrect for this scenario. DoH (DNS over HTTPS) secures DNS queries and is unrelated to IP address assignment.

SLAAC (Stateless Address Autoconfiguration) is used for IPv6, not IPv4 environments. APIPA (Automatic Private IP Addressing) assigns a link-local address when DHCP fails, but it does not provide consistent or routable addressing suitable for shared printers.

Therefore, configuring a DHCP reservation ensures consistent network access to the printer after power disruptions.

NEW QUESTION: 63

An administrator is setting up an SNMP server for use in the enterprise network and needs to create device IDs within a MIB. Which of the following describes the function of a MIB?

- A. DHCP relay device
- B. Policy enforcement point
- C. Definition file for event translation
- D. Network access controller

Answer: ([SHOW ANSWER](#))

* MIB (Management Information Base): A MIB is a database used for managing the entities in a communication network. The MIB is used by Simple Network Management Protocol (SNMP) to translate events into a readable format, enabling network administrators to manage and monitor network devices effectively.

* Function of MIB: MIBs contain definitions and information about all objects that can be managed on a network using SNMP. These objects are defined using a hierarchical namespace containing object identifiers (OIDs).

CompTIA Network+ materials discussing SNMP and MIB functionality.

NEW QUESTION: 64

A network administrator is implementing security zones for each department. Which of the following should the administrator use to accomplish this task?

A. ACLs

B. Port security

C. Content filtering

D. NAC

Answer: ([SHOW ANSWER](#))

* Understanding ACLs:

* Access Control Lists (ACLs): A set of rules used to control network traffic and restrict access to network resources by filtering packets based on IP addresses, protocols, or ports.

* Implementing Security Zones:

* Defining Zones: ACLs can be used to create security zones by applying specific rules to different departments, ensuring that only authorized traffic is allowed between these zones.

* Control Traffic: ACLs control inbound and outbound traffic at network boundaries, enforcing security policies and preventing unauthorized access.

* Comparison with Other Options:

* Port Security: Limits the number of devices that can connect to a switch port, preventing MAC address flooding attacks, but not used for defining security zones.

* Content Filtering: Blocks or allows access to specific content based on predefined policies, typically used for web filtering rather than network segmentation.

* NAC (Network Access Control): Controls access to the network based on the security posture of devices but does not define security zones.

* Implementation Steps:

* Define ACL rules based on the requirements of each department.

* Apply these rules to the appropriate network interfaces or firewall policies to segment the network into security zones.

References:

* CompTIA Network+ study materials on network security and access control methods.

NEW QUESTION: 65

Which of the following OSI model layers can utilize a connectionless protocol for data transmission?

A. Physical

B. Network

C. Transport

D. Application

Answer: ([SHOW ANSWER](#))

The Network layer (Layer 3 of the OSI model) can utilize the connectionless protocol IP (Internet Protocol) to send data packets independently without establishing a connection. This approach is typical for protocols like IP, which provide best-effort delivery rather than guaranteed delivery. The document explains:

"The OSI Network Layer is responsible for logical addressing and routing, and it can utilize connectionless protocols like IP to send packets without requiring a session setup. This layer does not guarantee packet delivery, relying on higher layers for error detection or correction if needed."

NEW QUESTION: 66

Which of the following is an example of a split-tunnel VPN?

- A. Only public resources are accessed through the user's internet connection.
- B. Encrypted resources are accessed through separate tunnels.
- C. All corporate and public resources are accessed through routing to on-site servers.
- D. ACLs are used to balance network traffic through different connections.

Answer: ([SHOW ANSWER](#))

In a split-tunnel VPN, only corporate traffic is sent through the VPN tunnel, while public internet traffic goes directly through the user's local ISP. This reduces bandwidth use on the corporate VPN concentrator and improves performance for non-work traffic.

- B). Separate tunnels for encrypted traffic describes multi-tunnel VPNs, not split tunneling.
- C). All traffic routed through on-site servers is a full-tunnel VPN, not split-tunnel.
- D). ACLs balancing traffic relates to routing or load balancing, not VPN split tunneling.

References (CompTIA Network+ N10-009):

Domain: Networking Concepts - VPN types, split vs. full tunnel, remote access.

NEW QUESTION: 67

A network administrator is managing network traffic so that classified services and applications are prioritized. Which of the following technologies should the network administrator use?

- A. Load balancing
- B. Time to live
- C. Quality of service
- D. Content delivery network

Answer: ([SHOW ANSWER](#))

Quality of Service (QoS) is used to prioritize certain types of traffic to ensure critical applications receive the bandwidth, low latency, and low jitter they need-especially during congestion. Network+ objectives cover QoS concepts such as classification, marking, queuing, and policing/shaping to manage how traffic is handled on interfaces and across links. If the requirement is to prioritize "classified services and applications," QoS policies can match traffic using ports, protocols, DSCP markings, VLAN tags, or application identifiers and then place that traffic into higher-priority queues or reserve bandwidth for it. Load balancing distributes traffic across multiple servers/paths but does not inherently prioritize one class of traffic over another on congested links. TTL (time to live) is an IP header field used to prevent routing loops and is unrelated to prioritization. A CDN improves content delivery and caching for distributed users, but it is not a traffic-prioritization mechanism within an organization's network. Therefore, QoS is the correct technology for prioritizing specific services and applications.

NEW QUESTION: 68

Which of the following routing technologies uses an attribute list for path selection?

- A. BGP
- B. RIP
- C. EIGRP
- D. OSPF

Answer: ([SHOW ANSWER](#))

BGP (Border Gateway Protocol) uses attributes like AS path, origin, and MED (multi-exit discriminator) to determine the best path among multiple available routes.

From Andrew Ramdayal's guide:

"BGP is the protocol underlying the global routing system of the internet. It is used for routing data between autonomous systems (ASes)... BGP uses a path vector mechanism and maintains a list of attributes for route selection."

NEW QUESTION: 69

A company is implementing a wireless solution in a high-density environment. Which of the following 802.11 standards is used when a company is concerned about device saturation and coverage?

- A. 802.11ac
- B. 802.11ax
- C. 802.11g
- D. 802.11n

Answer: ([SHOW ANSWER](#))

802.11ax, also known as Wi-Fi 6, is designed for high-density environments and improves device saturation and coverage compared to previous standards.

802.11ac: While it offers high throughput, it is not optimized for high-density environments as effectively as 802.11ax.

802.11ax (Wi-Fi 6): Introduces features like OFDMA, MU-MIMO, and BSS Coloring, which enhance performance in crowded environments, reduce latency, and increase the number of devices that can be connected simultaneously.

802.11g and 802.11n: Older standards that do not offer the same level of efficiency or support for high device density as 802.11ax.

Network References:

CompTIA Network+ N10-007 Official Certification Guide: Covers the 802.11 standards and their capabilities.

Cisco Networking Academy: Provides training on Wi-Fi technologies and best practices for high-density deployments.

Network+ Certification All-in-One Exam Guide: Discusses the various 802.11 standards and their applications in different environments.

NEW QUESTION: 70

A company wants to implement a disaster recovery site or non-critical appliance, which can tolerate a short period of downtime. Which of the following type of sites should the company implement to achieve this goal?

- A. Hot
- B. Cold
- C. Warm
- D. Passive

Answer: ([SHOW ANSWER](#))

A warm site is a compromise between a hot site and a cold site, providing a balance between cost and recovery time. It is partially equipped with the necessary hardware, software, and infrastructure, allowing for a quicker recovery compared to a cold site but at a lower cost than a hot site.

- * Recovery Time: Warm sites can be operational within hours to a day, making them suitable for non-critical applications that can tolerate short downtimes.

- * Cost-Effectiveness: Warm sites are more economical than hot sites as they do not require all systems to be fully operational at all times.

Network References:

- * CompTIA Network+ N10-007 Official Certification Guide: Discusses disaster recovery strategies and the different types of recovery sites.

- * Cisco Networking Academy: Provides training on disaster recovery planning and site selection.

- * Network+ Certification All-in-One Exam Guide: Explains the characteristics of hot, warm, and cold sites and their use cases in disaster recovery planning.

Warm sites offer a practical solution for maintaining business continuity for non-critical applications, balancing the need for availability with cost considerations.

NEW QUESTION: 71

After installing a series of Cat 8 keystones, a data center architect notices higher than normal interference during tests. Which of the following steps should the architect take to troubleshoot the issue?

A. Check to see if the end connections were wrapped in copper tape before terminating.

B. Use passthrough modular crimping plugs instead of traditional crimping plugs.

C. Connect the RX/TX wires to different pins.

D. Run a speed test on a device that can only achieve 100Mbps speeds.

Answer: ([SHOW ANSWER](#))

- * Importance of Proper Termination:

- * Cat 8 cabling requires precise termination practices to ensure signal integrity and reduce interference. One common requirement is to wrap the end connections in copper tape to maintain shielding and reduce electromagnetic interference (EMI).

- * Interference Troubleshooting:

- * Interference in high-frequency cables like Cat 8 can be caused by improper shielding or grounding. Checking the end connections for proper wrapping in copper tape is a crucial step.

- * Why Other Options are Less Likely:

- * Passthrough modular crimping plugs: Not specifically related to interference issues and are typically used for ease of cable assembly.

- * Connecting RX/TX wires to different pins: Would likely result in no connection or incorrect data transmission rather than interference.

- * Running a speed test on a device that can only achieve 100Mbps speeds: This would not diagnose interference and would not provide relevant information for Cat 8 cabling rated for higher speeds.

- * Corrective Actions:

- * Verify that all end connections are properly wrapped with copper tape before termination.

- * Ensure that the shielding is continuous and properly grounded throughout the installation.

- * Retest the cabling for interference after making corrections.

References:

- * CompTIA Network+ study materials and structured cabling installation guides.

NEW QUESTION: 72

Before using a guest network, an administrator requires users to accept the terms of use. Which of the following is the best way to accomplish this goal?

- A. Pre-shared key
- B. Autonomous access point
- C. Captive portal
- D. WPA2 encryption

Answer: ([SHOW ANSWER](#))

A captive portal is a web page that users must view and interact with before being granted access to a network. It is commonly used in guest networks to enforce terms of use agreements. When a user connects to the network, they are redirected to this portal where they must accept the terms of use before proceeding. This method ensures that users are aware of and agree to the network's policies, making it the best choice for this scenario. References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 73

A network administrator is deploying a new switch and wants to make sure that the default priority value was set for a spanning tree. Which of the following values would the network administrator expect to see?

- A. 4096
- B. 8192
- C. 32768
- D. 36684

Answer: ([SHOW ANSWER](#))

* Understanding Spanning Tree Protocol (STP):

* STP is used to prevent network loops in Ethernet networks by creating a spanning tree that selectively blocks some redundant paths.

* Default Priority Value:

* Bridge Priority: STP uses bridge priority to determine which switch becomes the root bridge. The default bridge priority value for most switches is 32768.

* Priority Range: The bridge priority can be set in increments of 4096, ranging from 0 to 61440.

* Configuration and Verification:

* When deploying a new switch, the network administrator can verify the bridge priority using commands such as `show spanning-tree` to ensure it is set to the default value of 32768.

* Comparison with Other Values:

* 4096 and 8192: Lower than the default priority, indicating these would be manually configured for higher preference.

* 36684: A non-standard value, likely a result of specific configuration changes.

References:

* CompTIA Network+ study materials on Spanning Tree Protocol and network configuration.

NEW QUESTION: 74

Which of the following terms describes the capability in a public cloud to add or remove compute resources based on need?

- A. Scalability
- B. Availability
- C. Elasticity
- D. Multitenancy

Answer: ([SHOW ANSWER](#))

The correct answer is C. Elasticity. In cloud computing, elasticity refers to the ability to increase or decrease resources quickly based on current demand. If workloads rise, more compute resources can be allocated. If demand drops, those resources can be reduced again. That is exactly what the question is describing.

This is slightly different from scalability. Scalability is the broader idea that a system can grow to handle more workload. Elasticity focuses more on the dynamic, on-demand adjustment of resources as conditions change. In exam questions, wording like "add or remove based on need" usually points straight to elasticity.

The other answer choices do not fit. Availability is about uptime and service access. Multitenancy refers to multiple customers sharing underlying cloud infrastructure while remaining logically separated. Neither describes rapid expansion and contraction of compute resources.

From a Network+ study perspective, elasticity is one of the core cloud characteristics to remember because it explains why cloud services are useful for workloads that are unpredictable or variable. Instead of permanently building for peak demand, organizations can consume more or less compute as required. That makes elasticity the best answer.

NEW QUESTION: 75

Which of the following ports should a network administrator enable for encrypted login to a network switch?

- A.** 22
- B.** 23
- C.** 80
- D.** 123

Answer: ([SHOW ANSWER](#))

Port 22 is used for Secure Shell (SSH), which enables encrypted remote login and command execution on network devices.

Port 23 = Telnet (unencrypted)

Port 80 = HTTP

Port 123 = NTP

From Andrew Ramdayal's guide:

"SSH uses port 22 to provide secure command-line access to devices such as switches and routers. Unlike Telnet (port 23), SSH encrypts session traffic, making it the preferred method for remote administration."

NEW QUESTION: 76

A network administrator needs to configure the core switches where multiple connections between data centers are used. Given the following requirements:

- * Fault tolerance and redundancy
- * Vendor interoperability
- * Increased bandwidth
- * Cost effectiveness
- * Simplified management

Which of the following should the administrator configure?

- A.** Spanning tree
- B.** Interface speeds to 10GB
- C.** Link aggregation
- D.** Jumbo frames

Answer: (SHOW ANSWER)

The best answer is C. Link aggregation. The requirements point directly to combining multiple physical links into one logical connection. Link aggregation provides higher total bandwidth, supports redundancy if one member link fails, and simplifies administration because the bundle is managed as a single logical interface instead of several separate ones.

Another important clue is vendor interoperability. Standards-based link aggregation, such as LACP, is designed to work across different vendors when supported properly. That makes it a strong match for inter- data-center switch environments where equipment may not all come from the same manufacturer.

The other choices do not satisfy the full requirement list. Spanning tree helps prevent loops, but it can block redundant links instead of actively using them for extra bandwidth. Setting interface speeds to 10GB increases speed per port, but it does not by itself provide the logical bundling, simplified management, or redundancy benefits described. Jumbo frames can improve efficiency for some traffic types, but they are not the right answer for bandwidth aggregation and resilient uplinks.

Because the question asks for a solution that improves throughput, keeps redundancy, remains cost effective, and is easier to manage, link aggregation is the strongest fit.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here: <https://www.edudump.com/exams/CompTIA/N10-009/premium/> (**608** Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 77

An IT department asks a newly hired employee to use a personal laptop until the company can provide one.

Which of the following policies is most applicable to this situation?

- A. IAM
- B. BYOD
- C. DLP
- D. AUP

Answer: (SHOW ANSWER)

BYOD (Bring Your Own Device) policies define rules for using personal devices on the company network.

Since the new employee is using a personal laptop, this policy applies.

Breakdown of Options:

- A). IAM (Identity and Access Management) - Governs user permissions, not device policies.
- B). BYOD (Bring Your Own Device) - # Correct answer. Covers using personal devices for work.
- C). DLP (Data Loss Prevention) - Focuses on preventing sensitive data leaks, not device usage policies.
- D). AUP (Acceptable Use Policy) - Covers internet and system usage, but not personal device rules.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 3.6: Explain security policies and best practices.

NEW QUESTION: 78

A network technician installs a new 19.7ft (6m), Cat 6, UTP cable for the connection between a server and a switch. Communication to the server is degraded, and the NIC statistics show dropped packets and CRC errors. Which of the following cables would the technician most likely use instead to reduce the errors?

- A. Coaxial cable
- B. 9.8ft (3m) cable
- C. Plenum cable
- D. STP cable

Answer: ([SHOW ANSWER](#))

The errors described - dropped packets and CRC (Cyclic Redundancy Check) errors - often indicate electromagnetic interference (EMI) on unshielded twisted pair (UTP) cabling. The correct replacement is STP (Shielded Twisted Pair), which has shielding that protects signals from external interference, ensuring better reliability in noisy environments such as data centers or near heavy electrical equipment.

A). Coaxial is not used for modern Ethernet server-switch links.

B). Shorter UTP cable does not solve EMI issues.

C). Plenum cable refers to cable jacket type for fire safety, not electrical shielding.

STP cabling reduces interference and ensures reliable gigabit+ Ethernet connections between servers and switches.

References (CompTIA Network+ N10-009):

Domain: Network Troubleshooting - Cabling issues, UTP vs. STP, EMI.

NEW QUESTION: 79

A network administrator needs to divide a Class B network into four equal subnets, each with a host range of 1,000 hosts. Which of the following subnet masks should the administrator use?

- A. 255.255.0.0
- B. 255.255.252.0
- C. 255.255.255.0
- D. 255.255.255.128

Answer: ([SHOW ANSWER](#))

The best answer is B. 255.255.252.0 , which is a /22 mask. A Class B network starts with a default mask of 255.255.0.0 or /16 . The question says the administrator wants four equal subnets , which means borrowing 2 bits from the host portion, since 2 borrowed bits gives $2^2 = 4$ subnets . That moves the mask from /16 to /18 if subnetting is based only on splitting the Class B into four equal parts. However, the answer choices point toward the host requirement as the deciding factor. Each subnet needs to support about 1,000 hosts . A /22 leaves 10 host bits , which gives $2^{10} = 1024$ total addresses , or 1022 usable hosts after subtracting the network and broadcast addresses. That fits the requirement. Among the options provided, 255.255.252.0 is the only mask that supports around 1,000 hosts per subnet.

The smaller masks, /24 and /25 , do not allow enough hosts. The default Class B mask, /16 , does not subnet the network at all. Based on the available choices and the host-capacity requirement, 255.255.252.0 is the correct exam answer.

NEW QUESTION: 80

A technician is plugging an Ethernet cable into a switch to bring a new device online, but the device is not showing an active network connection. Previously, another technician turned off unused switchports as part of device hardening. Which of the following describes the port status?

- A. Error disabled
- B. Idle

- C. Suspended
- D. Administratively down

Answer: ([SHOW ANSWER](#))

The correct answer is D. Administratively down . The question states that another technician had already turned off unused switchports as part of hardening. When a port is intentionally disabled by configuration, its status is described as administratively down . In other words, the switchport is not broken and has not failed on its own; it has simply been shut down by an administrator.

This is a common security practice. Unused ports are often disabled so unauthorized devices cannot be plugged in and gain access to the network. If a legitimate device later needs that port, the administrator must re-enable it before the link can come up.

The other answer choices do not line up as well with the scenario. Error disabled usually points to a protective shutdown caused by a violation or fault, such as port security or BPDU guard. Idle is not the standard description for a manually shut switchport in this context. Suspended can appear with certain switch features, but it is not the normal label for a port deliberately turned off as part of hardening.

The phrase "turned off unused switchports" is the key detail. That clearly indicates a manual administrative shutdown, so administratively down is the best answer.

NEW QUESTION: 81

A network administrator recently updated configurations on a Layer 3 switch. Following the updates, users report being unable to reach a specific file server. Which of the following is the most likely cause?

- A. Incorrect ACLs
- B. Switching loop
- C. Duplicate IP addresses
- D. Wrong default route

Answer: ([SHOW ANSWER](#))

*Since this issue occurred after a configuration change on a Layer 3 switch, the most likely cause is misconfigured ACLs (Access Control Lists).

*ACLs control which traffic is allowed or denied, so an incorrect ACL may be blocking access to the file server.

*Why not the other options?

*Switching loop (B): A switching loop occurs at Layer 2 (not Layer 3) and causes network-wide broadcast storms, not just loss of access to a file server.

*Duplicate IP addresses (C): This would cause connectivity issues for the devices with the conflict, but not necessarily prevent all users from accessing the file server.

*Wrong default route (D): The default route is used for traffic leaving the local network. If users are unable to access an internal file server, this is unlikely to be the issue.

Reference:

CompTIA Network+ (N10-009) Official Guide - Chapter 8: Network Access Control and ACLs

NEW QUESTION: 82

A company experiences an incident involving a user who connects an unmanaged switch to the network.

Which of the following technologies should the company implement to help avoid similar incidents without conducting an asset inventory?

- A. Screened subnet
- B. 802.1X
- C. MAC filtering
- D. Port security

Answer: ([SHOW ANSWER](#))

Port security is a Layer 2 security feature that restricts the number of devices connecting to a network switch port. It helps prevent unauthorized devices, such as an unmanaged switch, from being connected to the network.

How Port Security Works:

Limits the number of MAC addresses that can connect to a port.

Can shut down or restrict the port if an unauthorized device is detected.

Prevents users from plugging in unauthorized networking equipment (e.g., unmanaged switches, hubs).

Incorrect Options:

A). Screened Subnet: A screened subnet (DMZ) is used for isolating external-facing servers, not for controlling unauthorized network connections.

B). 802.1X: Provides authentication for devices but requires a RADIUS server, which is a more complex solution than port security.

C). MAC Filtering: Controls which MAC addresses can connect but is difficult to manage and can be spoofed.

Reference:

CompTIA Network+ N10-009 Official Study Guide - Chapter on Network Security Controls

NEW QUESTION: 83

Which of the following kinds of targeted attacks uses multiple computers or bots to request the same resource repeatedly?

A. On-path

B. DDoS

C. ARP spoofing

D. MAC flooding

Answer: ([SHOW ANSWER](#))

A Distributed Denial of Service (DDoS) attack leverages multiple computers or bots (botnet) to flood a target system with requests, overwhelming its resources and making it unavailable to legitimate users. This is a common tactic used by attackers to disrupt services. The document explains:

"A DDoS (Distributed Denial of Service) attack involves multiple computers (often called bots) simultaneously sending requests to a single resource, overwhelming the system and causing a denial of service to legitimate users."

NEW QUESTION: 84

In the troubleshooting methodology, which of the following actions comes after verifying that the initial problem has been resolved?

A. If necessary, escalating the issue

B. Attempting to replicate the problem

C. Documenting findings

D. Implementing the plan

Answer: ([SHOW ANSWER](#))

In the CompTIA Network+ (N10-009) troubleshooting methodology, the step that follows verifying full system functionality (confirming the issue is resolved and validating with the user/requirements) is documenting findings, actions, and outcomes. Documentation is a required closing step because it captures what the original symptoms were, what troubleshooting steps were performed, what root cause was identified (if found), what remediation was applied, and what validation confirmed success. This record supports operational continuity by enabling faster resolution if the issue recurs, improving knowledge transfer across teams, and meeting organizational change-control or compliance requirements.

The other options fall in different parts of the methodology. Attempting to replicate the problem is typically performed earlier-after identifying symptoms and before or during isolation-to confirm the issue and help narrow scope. Implementing the plan occurs before verification; you

implement the selected solution or escalation plan and then test/verify. Escalating the issue occurs when the technician lacks access, expertise, time, or evidence to proceed, and it can happen during troubleshooting-but it is not the standard step that comes after verifying resolution.

NEW QUESTION: 85

Which of the following involves an attacker traversing from one part of a network to another part that should be inaccessible?

- A. MAC flooding
- B. DNS poisoning
- C. VLAN hopping
- D. ARP spoofing

Answer: (SHOW ANSWER)

VLAN hopping allows an attacker to send traffic into another VLAN without authorization, often by impersonating a switch and negotiating a trunk link. This lets the attacker traverse into normally inaccessible VLANs.

- A). MAC flooding disrupts switch operations but does not cross VLANs.
- B). DNS poisoning corrupts name resolution.
- D). ARP spoofing reroutes local traffic but doesn't grant VLAN traversal.

References (CompTIA Network+ N10-009):

Domain: Network Security - VLAN attacks, unauthorized lateral movement.

NEW QUESTION: 86

Users cannot connect to an internal website with an IP address 10.249.3.76. A network administrator runs a command and receives the following output:

```
1 3ms 2ms 3ms 192.168.25.234
2 2ms 3ms 1ms 192.168.3.100
3 4ms 5ms 2ms 10.249.3.1
4 *
5 '
6 *
7 *
```

Which of the following command-line tools is the network administrator using?

- A. tracert
- B. netstat
- C. tcpdump
- D. nmap

Answer: (SHOW ANSWER)

* Understanding Tracert:

* tracert(Traceroute in Windows) is a command-line tool used to trace the path that packets take from the source to the destination. It records the route (the specific gateways at each hop) and measures transit delays of packets across an IP network.

* Output Analysis:

* The output shows a series of IP addresses with corresponding round-trip times (RTTs) in milliseconds.

* The asterisks (*) indicate that no response was received from those hops, which is typical for routers or firewalls that block ICMP packets used by tracert.

* Comparison with Other Tools:

* netstat:Displays network connections, routing tables, interface statistics, and more, but does not trace packet routes.

* tcpdump:Captures network packets for analysis, used for detailed network traffic inspection.

* nmap:A network scanning tool used to discover hosts and services on a network, not for tracing packet routes.

* Usage:

* tracerthelps identify the path to a destination and locate points of failure or congestion in the network.

References:

* CompTIA Network+ study materials on network troubleshooting and diagnostic tools.

NEW QUESTION: 87

Which of the following network traffic types is sent to all nodes on the network?

A. Unicast

B. Broadcast

C. Multicast

D. Anycast

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (aligned to N10-009):

A broadcast message is delivered to all nodes in a broadcast domain (e.g., ARP requests).

A). Unicast is one-to-one.

C). Multicast is one-to-many but only to subscribed members.

D). Anycast is one-to-one-of-many, sending to the nearest node.

References (CompTIA Network+ N10-009):

Domain: Networking Concepts - Traffic types: unicast, multicast, broadcast, anycast.

NEW QUESTION: 88

A systems administrator is looking for operating system information, running services, and network ports that are available on a server. Which of the following software tools should the administrator use to accomplish this task?

A. Nmap

B. Traceroute

C. Netstat

D. Ping

Answer: ([SHOW ANSWER](#))

The correct answer is A. Nmap. Nmap (Network Mapper) is a powerful network scanning and reconnaissance tool specifically designed to gather detailed information about hosts on a network. According to CompTIA Network+ N10-009 objectives, Nmap can be used to identify open ports, running services, and even the operating system of a target device through techniques such as TCP/UDP scanning and OS fingerprinting.

This makes Nmap the best choice when a systems administrator needs a comprehensive view of a server's exposure and configuration. It can enumerate services (e.g., HTTP, SSH), detect service versions, and determine which ports are open, closed, or filtered.

The other options are more limited in scope. Traceroute is used to map the path packets take across a network and identify latency or routing issues, but it does not provide service or OS details. Netstat shows active connections and listening ports on a local machine but does not perform remote OS detection or full service enumeration. Ping simply tests connectivity and reachability using ICMP and does not provide detailed system information.

Therefore, Nmap is the most appropriate and comprehensive tool for this requirement.

NEW QUESTION: 89

A customer wants to separate the finance department from the marketing department. The network administrator suggests segmenting the existing Class C network into two sections and readdressing all devices appropriately. Which of the following subnet masks should the network administrator use?

- A. /24
- B. /25
- C. /26
- D. /27

Answer: ([SHOW ANSWER](#))

The correct answer is /25, which is the appropriate subnet mask for dividing an existing Class C network into two equal subnets. According to the CompTIA Network+ N10-009 objectives, subnetting is a core networking concept used to improve network segmentation, performance, and security.

A Class C network uses a default subnet mask of /24 (255.255.255.0), which provides 256 total addresses (254 usable). To split this network into two sections, the administrator must borrow one host bit from the last octet. Borrowing one bit results in a /25 subnet mask (255.255.255.128).

This creates two subnets, each with

128 total addresses (126 usable)-an ideal solution for separating two departments such as finance and marketing.

A /24 would not create any segmentation, as it represents the original single network. A /26 would create four subnets, and a /27 would create eight subnets, both of which exceed the requirement of only two sections and unnecessarily reduce the number of available host addresses per subnet.

The Network+ objectives emphasize selecting subnet masks based on organizational requirements, balancing the number of subnets with sufficient host capacity. In this scenario, /25 is the most efficient and correct choice.

NEW QUESTION: 90

Which of the following is an advantage of using an IDS over an IPS?

- A. An IDS requires less processing power to analyze traffic
- B. An IDS is less disruptive during the initial deployment of the technology
- C. An IDS is easier to restrict access
- D. An IDS is more accurate due to fewer false positives

Answer: ([SHOW ANSWER](#))

An IDS is less disruptive during initial deployment because it is normally deployed out of band or passively.

An intrusion detection system monitors traffic and generates alerts when suspicious or malicious activity is detected. Since it does not usually sit inline between the source and destination, it can observe network activity without directly blocking production traffic. This makes IDS deployment safer during testing, tuning, and baselining.

The CompTIA Network+ N10-009 objectives include network security appliances, monitoring, detection, prevention, and operational impact. An IPS, or intrusion prevention system, is usually inline and can actively block, drop, or reset traffic. While that provides stronger prevention capability, it also creates a higher risk of disrupting legitimate traffic if signatures, rules, or thresholds are misconfigured.

An IDS does not necessarily require less processing power because it still analyzes traffic and may inspect large volumes of data. It is not inherently easier to restrict access, and it is not automatically more accurate than an IPS. Both IDS and IPS technologies can experience false positives depending on tuning and signatures. Therefore, the best advantage of IDS over IPS is lower disruption during initial deployment.

NEW QUESTION: 91

A network administrator is notified that a user cannot access resources on the network. The network administrator checks the physical connections to the workstation labeled User 3 and sees the Ethernet is properly connected. However, the network interface's indicator lights are not blinking on either the computer or the switch. Which of the following is the most likely cause?

- A. The switch failed.
- B. The default gateway is wrong.
- C. The port is shut down.
- D. The VLAN assignment is incorrect.

Answer: (SHOW ANSWER)

When a network interface's indicator lights are not blinking on either the computer or the switch, it suggests a physical layer issue. Here is the detailed reasoning:

- * Ethernet Properly Connected: The Ethernet cable is correctly connected, eliminating issues related to a loose or faulty cable.
- * No Indicator Lights: The absence of blinking indicator lights on both the computer and the switch typically points to the port being administratively shut down.
- * Switch Port Shut Down: In networking, a switch port can be administratively shut down, disabling it from passing any traffic. This state is configured by network administrators and can be verified and changed using the command-line interface (CLI) of the switch.

Command to Check and Enable Port:

```
bash
```

Copy code

```
Switch> enable
```

```
Switch# configure terminal
```

```
Switch(config)# interface [interface id]
```

```
Switch(config-if)# no shutdown
```

- * The command no shutdown re-enables the interface if it was previously disabled. This will restore the link and the indicator lights should start blinking, showing activity.

Basic Configuration Commands PDF, sections on interface configuration (e.g., shutdown, no shutdown).

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here: <https://www.edudump.com/exams/CompTIA/N10-009/premium/> (608 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 92

Computer A cannot reach Computer B in the following network:

Computer A: 172.16.2.10/16

Computer B: 172.16.4.10/16

Switch A:

Gi0/1 access VLAN 1, status up/up

Gi0/9 access VLAN 8, status up/up

Gi0/10 access VLAN 5, status administratively down

Switch B:

Gi0/1 access VLAN 1, status up/up

Gi0/9 access VLAN 8, status up/up

Gi0/10 access VLAN 5, status administratively down

Which of the following will resolve the issue?

A. Set up link aggregation between Switch A and Switch B on Gi0/9 and Gi0/10

B. Configure spanning tree on Switch A and Switch B

C. Establish a trunk connection between Switch A and Switch B

D. Put Computer A and Computer B in the same /24 subnet

Answer: (SHOW ANSWER)

The correct solution is to establish a trunk connection between Switch A and Switch B. Computer A and Computer B are both connected to access VLAN 1 on their local switches. However, the inter-switch link appears to be configured as an access port in VLAN 8. Because the link between the switches is not carrying VLAN 1 traffic, devices in VLAN 1 on separate switches cannot communicate across that connection.

The CompTIA Network+ N10-009 objectives include VLANs, switching, trunking, access ports, and troubleshooting Layer 2 connectivity. Access ports carry traffic for a single VLAN. Trunk ports carry traffic for multiple VLANs between switches, usually using tagging such as IEEE 802.1Q. To allow VLAN 1 devices on both switches to communicate, the inter-switch connection must carry VLAN 1 traffic. A trunk would allow VLAN 1 and other required VLANs to pass between the switches.

Link aggregation is not the issue, and Gi0/10 is administratively down. Spanning Tree Protocol prevents loops but does not fix missing VLAN transport. Changing both hosts to a /24 would not solve the VLAN separation problem and could make IP reachability worse. Therefore, trunking is required.

NEW QUESTION: 93

Users in a new subnet segment are unable to get IP addresses from the DHCP server. A network administrator notices that the DHCP server is located on a remote segment. Which of the following should the administrator do to resolve the issue?

A. Configure the IP helper on the network device

B. Configure the switch to accept EAPoL on the new VLAN segment

C. Configure the existing DHCP lease time

D. Configure the DHCP server to operate on non-standard ports

Answer: (SHOW ANSWER)

The administrator should configure an IP helper address on the network device. DHCP clients initially use broadcast messages to discover a DHCP server. Routers do not forward broadcasts by default, so if the DHCP server is located on a different subnet, clients in the new subnet will not be able to reach it unless DHCP relay is configured. An IP helper address allows the router or Layer 3 switch interface to forward DHCP requests from the client subnet to the remote DHCP server as unicast traffic.

The CompTIA Network+ N10-009 objectives include DHCP, IP addressing, VLANs, routing, and troubleshooting network services. DHCP relay is a common requirement in networks with multiple VLANs or subnets that use centralized DHCP servers.

EAPoL is related to 802.1X authentication and does not solve DHCP relay across routed segments. Changing DHCP lease time affects how long clients keep assigned addresses, but it does not help clients reach a remote DHCP server. DHCP uses standard ports UDP 67 and UDP 68, and changing to non-standard ports would create more problems. Therefore, configuring an IP helper is the correct solution.

NEW QUESTION: 94

A network engineer needs to change, update, and control APs remotely, with real-time visibility over HTTPS.

Which of the following will best allow these actions?

- A.** Web interface
- B.** Command line
- C.** SNMP console
- D.** API gateway

Answer: ([SHOW ANSWER](#))

API gateways offer programmable control and real-time communication, commonly over HTTPS, which allows administrators to update and manage devices like access points remotely and efficiently.

From Andrew Ramdayal's guide:

"APIs enable automation and real-time interaction with network devices via secure interfaces, often using HTTPS for encrypted communication and control."

NEW QUESTION: 95

A network engineer is implementing a new connection between core switches. The engineer deploys the following configurations:

Core-SW01

vlan 100

name

interface Ethernet 1/1

channel-group 1 mode active

interface Ethernet 1/2

channel-group 1 mode active

interface port-channel 1

switchport mode trunk

switchport trunk allow vlan 100

Core-SW02

vlan 100

name

interface Ethernet 1/1

switchport mode trunk

switchport trunk allow vlan 100

interface Ethernet 1/2

switchport mode trunk

switchport trunk allow vlan 100

interface port-channel 1

switchport mode trunk

switchport trunk allow vlan 100

Which of the following is the state of the Core-SW01 port-channel interfaces?

- A.** Incrementing CRC errors
- B.** Error disabled

C. Administratively down

D. Suspended

Answer: ([SHOW ANSWER](#))

On Core-SW01, the ports are configured with LACP (mode active) for link aggregation. On Core-SW02, the ports are configured as independent trunks, not as part of an LACP group. Because of this mismatch, LACP cannot form the bundle, and the aggregated ports on SW01 will go into a suspended state.

A). CRC errors suggest cabling or signal integrity issues, not config mismatch.

B). Error disabled occurs when a violation (like BPDU guard or port security) disables the port, not LACP mismatch.

C). Administratively down indicates a shutdown command, not the case here.

References (CompTIA Network+ N10-009):

Domain: Network Troubleshooting - Port-channel/LACP configuration issues, interface states.

NEW QUESTION: 96

A network manager wants to implement a SIEM system to correlate system events. Which of the following protocols should the network manager verify?

A. NTP

B. DNS

C. LDAP

D. DHCP

Answer: ([SHOW ANSWER](#))

* Role of NTP (Network Time Protocol):

* NTP is used to synchronize the clocks of network devices to a reference time source. Accurate time synchronization is critical for correlating events and logs from different systems.

* Importance for SIEM Systems:

* Event Correlation: SIEM (Security Information and Event Management) systems collect and analyze log data from various sources. Accurate timestamps are essential for correlating events across multiple systems.

* Time Consistency: Without synchronized time, it is challenging to piece together the sequence of events during an incident, making forensic analysis difficult.

* Comparison with Other Protocols:

* DNS (Domain Name System): Translates domain names to IP addresses but is not related to time synchronization.

* LDAP (Lightweight Directory Access Protocol): Used for directory services, such as user authentication and authorization.

* DHCP (Dynamic Host Configuration Protocol): Assigns IP addresses to devices on a network but does not handle time synchronization.

* Implementation:

* Ensure that all network devices, servers, and endpoints are synchronized using NTP. This can be achieved by configuring devices to use an NTP server, which could be a local server or an external time source.

References:

* CompTIA Network+ study materials on network protocols and SIEM systems.

NEW QUESTION: 97

Company C is acquiring Company A and Company B. Company C needs to merge all three networks into one Class B network. Additionally, the network capacity of each company needs to grow by 20%. Company C also requires segmentation of Company A and Company B to account for unknown security vulnerabilities within each.

Instructions:

Select the correct subnet range to meet Company C ' s requirements.

Company	Current number of devices	Current subnet range	New subnet range
A	32	192.168.10.1/27	Select
			192.168.10.0/22
			10.0.8.0/26
			192.168.10.0/27
			10.0.1.0/21
			192.168.10.0/26
			10.0.0.1/17
			10.0.0.1/18
			192.168.1.0/23
			192.168.1.0/22
			10.0.1.0/22
			10.0.8.0/27
B	100	192.168.1.1/22	Select
			192.168.10.0/27
			10.0.1.0/22
			192.168.1.0/23
			10.0.0.1/17
			192.168.1.0/22
			10.0.8.0/27
			10.0.8.0/26
			10.0.0.1/18
			192.168.10.0/26
			192.168.10.0/22
			10.0.1.0/21
C	10,000	10.0.0.1/8	Select
			192.168.10.0/27
			10.0.1.0/22
			192.168.1.0/23
			10.0.0.1/17
			192.168.1.0/22
			10.0.8.0/27
			10.0.8.0/26
			10.0.0.1/18
			192.168.10.0/26
			192.168.10.0/22
			10.0.1.0/21

Answer:

Company	Current number of devices	Current subnet range	New subnet range
A	32	192.168.10.1/27	Select 192.168.10.0/22 10.0.8.0/26 192.168.10.0/27 10.0.1.0/21 192.168.10.0/26 10.0.0.1/17 10.0.0.1/18 192.168.1.0/23 192.168.1.0/22 10.0.1.0/22 10.0.8.0/27
B	100	192.168.1.1/22	Select 192.168.10.0/27 10.0.1.0/22 192.168.1.0/23 10.0.0.1/17 192.168.1.0/22 10.0.8.0/27 10.0.8.0/26 10.0.0.1/18 192.168.10.0/26 192.168.10.0/22 10.0.1.0/21
C	10,000	10.0.0.1/8	Select 192.168.10.0/27 10.0.1.0/22 192.168.1.0/23 10.0.0.1/17 192.168.1.0/22 10.0.8.0/27 10.0.8.0/26 10.0.0.1/18 192.168.10.0/26 192.168.10.0/22 10.0.1.0/21

Explanation:

A = 192.168.10.0/26

B = 192.168.1.0/23

C = 10.0.0.1/18

Using the choices shown in the screenshot, the best-fit subnet selections are based on host growth requirements first, then segmentation.

For Company A, the current device count is 32. With 20% growth, that becomes about 39 devices. A /27 only supports 30 usable hosts, so it is too small. A /26 supports 62 usable hosts, so 192.168.10.0/26 is the correct choice.

For Company B, the current device count is 100. With 20% growth, that becomes 120 devices. The smallest correct subnet would normally be a /25 with 126 usable hosts, but that option is not shown. From the available choices, 192.168.1.0/23 is the smallest subnet that still supports more than 120 hosts, so that is the best answer.

For Company C, the current device count is 10,000. With 20% growth, it needs space for 12,000 hosts. A /18 provides 16,382 usable hosts, while a /19 is not available and a /21 or /22 would be far too small. Therefore, 10.0.0.1/18 is the correct selection.

One important note: the dropdown choices shown do not actually let all three companies be placed into a single true Class B network block. So these answers are the best valid selections from the provided options.

NEW QUESTION: 98

A network engineer connects a business to a new ISP. A simple ping test to 8.8.8.8 is successful. However, users complain of extreme slowness to any website and periods of no connectivity. Which of the following is the most likely cause?

- A. Incorrect default gateway
- B. VLAN mismatch
- C. Subnet mask configuration
- D. Duplicate ISP IP address

Answer: (SHOW ANSWER)

If the business shares or duplicates the ISP-assigned public IP address, routing instability and conflicts will occur. Pinging a public IP like 8.8.8.8 may work (since ICMP can bypass certain conflicts), but browsing websites (which requires stable sessions and return traffic) will fail intermittently.

- A). If the default gateway were incorrect, no external connectivity would work at all.
- B). VLAN mismatch is an internal issue, not affecting ISP routing.
- C). Subnet mask misconfiguration would prevent consistent routing but usually blocks ping too.

References (CompTIA Network+ N10-009):

Domain: Network Troubleshooting - Internet connectivity issues, ISP IP conflicts.

NEW QUESTION: 99

A network administrator has been monitoring the company's servers to ensure that they are available. Which of the following should the administrator use for this task?

- A. Packet capture
- B. Data usage reports
- C. SNMP traps
- D. Configuration monitoring

Answer: (SHOW ANSWER)

To monitor server availability, SNMP traps are the best choice. SNMP (Simple Network Management Protocol) allows devices to send alerts (traps) when certain conditions are met, such as server downtime or high resource usage.

Breakdown of Options:

- A). Packet capture - Capturing packets provides insights into network traffic but does not actively monitor server availability.
- B). Data usage reports - These analyze network traffic consumption but do not indicate whether a server is available or not.

C). SNMP traps - Correct answer. SNMP traps notify administrators of server issues in real time.

D). Configuration monitoring - This tracks configuration changes rather than availability.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 2.3: Explain network monitoring concepts.

RFC 1157: Simple Network Management Protocol (SNMP)

NEW QUESTION: 100

Which of the following are environmental factors that should be considered when installing equipment in a building? (Select two).

A. Fire suppression system

B. UPS location

C. Humidity control

D. Power load

E. Floor construction type

F. Proximity to nearest MDF

Answer: ([SHOW ANSWER](#))

When installing equipment in a building, environmental factors are critical to ensure the safety and longevity of the equipment. A fire suppression system is essential to protect the equipment from fire hazards. Humidity control is crucial to prevent moisture-related damage, such as corrosion and short circuits, which can adversely affect electronic components. Both factors are vital for maintaining an optimal environment for networking equipment. References: CompTIA Network+ study materials.

NEW QUESTION: 101

Which of the following has the highest administrative distance?

A. Enhanced Interior Gateway Routing Protocol

B. Border Gateway Protocol

C. Static route

D. Open Shortest Path First

Answer: ([SHOW ANSWER](#))

Border Gateway Protocol is the best answer when considering BGP's internal administrative distance value.

Administrative distance is used by routers to decide which route source is more trustworthy when multiple routing sources advertise a path to the same destination. Lower values are preferred. A static route normally has an administrative distance of 1, internal EIGRP is commonly 90, OSPF is 110, external EIGRP is 170, external BGP is 20, and internal BGP is 200.

The CompTIA Network+ N10-009 objectives include routing protocol behavior, dynamic routing, route selection, and administrative distance.

Because internal BGP has an administrative distance of 200, BGP can have the highest administrative distance among the listed options.

This question is slightly tricky because BGP has different administrative distance values depending on whether the route is learned through external BGP or internal BGP. If a question specifically said external BGP, its value would be 20, which would not be the highest. However, among the listed technologies, BGP is the best exam-style answer because iBGP has the highest default administrative distance listed here.

NEW QUESTION: 102

A support agent receives a report that a remote user's wired devices are constantly disconnecting and have slow speeds. Upon inspection, the support agent sees that the user's coaxial modem has a signal power of -97 dB.

- A. Removing any splitters connecte to the line
- B. Switching the devices to wireless
- C. Moving the devices closer to the modern
- D. Lowering the network speed

Answer: ([SHOW ANSWER](#))

A signal power of -97dB indicates a very weak signal, which can cause connectivity issues and slow speeds.

Splitters on a coaxial line can degrade the signal quality further, so removing them can help improve the signal strength and overall connection quality.

- * Signal Quality: Splitters can reduce the signal strength by dividing the signal among multiple lines, which can be detrimental when the signal is already weak.
- * Direct Connection: Ensuring a direct connection from the modem to the incoming line can maximize signal quality and reduce potential points of failure.

Network References:

- * CompTIA Network+ N10-007 Official Certification Guide: Discusses troubleshooting connectivity issues and the impact of signal strength on network performance.
- * Cisco Networking Academy: Provides insights on maintaining optimal signal quality in network setups.
- * Network+ Certification All-in-One Exam Guide: Covers common network issues, including those related to signal degradation and ways to mitigate them.

NEW QUESTION: 103

An administrator needs to configure an IoT device with a /21 subnet mask, but the device will only accept dotted decimal notation. Which of the following subnet masks should the administrator use?

- A. 255.255.224.0
- B. 255.255.240.0
- C. 255.255.248.0
- D. 255.255.252.0

Answer: ([SHOW ANSWER](#))

A /21 subnet mask means 21 bits are network bits:

$8 + 8 + 5 = 21$ # leaves 11 bits for hosts.

Subnet mask in binary: 11111111.11111111.11111000.00000000

Converted to decimal: 255.255.248.0

Therefore:

- A). /19 = 255.255.224.0
- B). /20 = 255.255.240.0
- # C. /21 = 255.255.248.0 # correct
- D). /22 = 255.255.252.0

Answer correction: The correct option is C. 255.255.248.0, not B.

References (CompTIA Network+ N10-009):

Domain: Networking Concepts - Subnetting, CIDR notation, dotted decimal masks.

NEW QUESTION: 104

Which of the following most likely determines the size of a rack for installation? (Select two).

- A. KVM size
- B. Switch depth
- C. Hard drive size
- D. Cooling fan speed
- E. Outlet amperage
- F. Server height

Answer: (SHOW ANSWER)

Understanding Rack Size Determination:

The size of a rack for installation is determined by the dimensions of the equipment to be housed in it, primarily focusing on the depth and height of the devices.

Switch Depth:

Depth of Equipment: The depth of network switches and other rack-mounted devices directly influences the depth of the rack. If the equipment is deeper, a deeper rack is required to accommodate it.

Industry Standards: Most racks come in standard depths, but it is essential to match the depth of the rack to the deepest piece of equipment to ensure proper fit and airflow.

Server Height:

Height of Equipment: The height of servers and other devices is measured in rack units (U), where 1U equals 1.75 inches. The total height of all equipment determines the overall height requirement of the rack.

Rack Units: A rack's height is typically described in terms of the number of rack units it can accommodate, such as 42U, 48U, etc.

Why Other Options are Less Relevant:

KVM Size: While important for management, KVM (Keyboard, Video, Mouse) switches do not typically determine rack size.

Hard Drive Size: Individual hard drives are installed within servers or storage devices, not directly influencing rack dimensions.

Cooling Fan Speed: Fan speed affects cooling but not the physical size of the rack.

Outlet Amperage: Power requirements do not determine rack dimensions but rather the electrical infrastructure supporting the rack.

References:

CompTIA Network+ study materials on rack installation and equipment sizing.

NEW QUESTION: 105

A network administrator needs to deploy a subnet using an IP address range that can support at least 260 devices with the fewest wasted addresses. Which of the following subnets should the administrator use?

- A. 172.16.0.0/24
- B. 172.25.2.0/23
- C. 172.30.1.0/22
- D. 172.33.0.0/21

Answer: (SHOW ANSWER)

To support at least 260 hosts, you need at least 512 total IP addresses (accounting for network/broadcast overhead).

/23 (255.255.254.0) gives 510 usable IPs, ideal for 260 devices with minimal waste.

/24 (255.255.255.0) gives only 254 usable - not enough.

/22 (1022 usable) and /21 (2046 usable) would work but result in significant address waste.

Reference:

CompTIA Network+ N10-009 Official Objectives: 2.1 - Given a scenario, configure and apply IP addressing schemes.

NEW QUESTION: 106

Which of the following routing protocols is most commonly used to interconnect WANs?

- A. IGP
- B. EIGRP
- C. BGP
- D. OSPF

Answer: ([SHOW ANSWER](#))

Border Gateway Protocol (BGP): BGP is the most commonly used routing protocol for interconnecting WANs, especially across the internet. It is used for exchanging routing information between autonomous systems (AS), making it the backbone protocol for large-scale WANs.

IGP (A): Interior Gateway Protocols like OSPF and EIGRP are typically used within a single AS, not between them.

EIGRP (B): While it is efficient, EIGRP is primarily used for intra-domain routing and not ideal for WAN interconnection.

OSPF (D): While OSPF can be used for WANs, it is not as common as BGP for inter-AS communication.

Reference: CompTIA Network+ Official Study Guide, Domain 1.3 (WAN Concepts), Domain 2.5 (Routing Protocols).

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here: <https://www.edudump.com/exams/CompTIA/N10-009/premium/> (608 Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 107

Which of the following network cables involves bounding light off of protective cladding?

- A. Twinaxial
- B. Coaxial
- C. Single-mode
- D. Multimode

Answer: ([SHOW ANSWER](#))

Multimode fiber optic cables involve the transmission of light signals that bounce off the core's cladding as they travel down the fiber. This characteristic differentiates it from single-mode fiber, where the light travels directly down the fiber without reflecting off the cladding.

Here are some detailed points about multimode fiber cables:

Construction: Multimode fibers have a larger core diameter, typically 50 or 62.5 microns, compared to single-mode fibers, which have a core diameter of about 9 microns.

Light Propagation: The larger core of multimode fiber allows multiple light modes to propagate. These modes travel at different angles, leading to reflections off the core-cladding boundary.

Distance and Bandwidth: Due to modal dispersion, where different light modes arrive at the receiver at different times, multimode fibers are suited for shorter distance applications compared to single-mode fibers.

Typical distances are up to 550 meters for 10 Gbps Ethernet using OM4 multimode fiber.

Applications: Multimode fibers are commonly used in LANs (Local Area Networks), data centers, and for shorter distance data transmission due to their cost-effectiveness and ease of installation.

Network References:

CompTIA Network+ N10-007 Official Certification Guide, which covers fiber optic technologies, including the differences between multimode and single-mode fibers.

Cisco Networking Academy: Provides training materials and reference guides on the properties of different fiber optic cables.

Fiber Optic Association (FOA): A professional society dedicated to fiber optics, offering extensive information and certification on fiber optic technologies.

Multimode fibers are specifically designed for short-range communication with higher data rates and are typically used in environments like data centers, where high bandwidth over shorter distances is crucial. The reflections off the cladding, inherent to multimode fiber, facilitate this high-capacity communication.

NEW QUESTION: 108

A help desk technician receives a report that users cannot access internet URLs. The technician performs ping tests and finds that sites fail when a URL is used but succeed when an IP is used. Which of the following tools should the technician utilize next?

A. tcpdump

B. tracert

C. nmap

D. dig

Answer: (SHOW ANSWER)

The issue is clearly related to DNS resolution, as IP-based connections succeed but domain name-based ones fail.

* D. dig(Domain Information Groper) is a DNS lookup tool used to troubleshoot DNS problems by querying name servers directly.

Other tools are less relevant here:

* A. tcpdump is a packet analyzer and is more advanced for deeper traffic analysis.

* B. tracert is used to trace the route to a destination, not ideal for DNS issues.

* C. nmap is a port scanner and network mapper, not for resolving DNS problems.

#Reference:

CompTIA Network+ N10-009 Official Objectives: 5.1 - Given a scenario, use the appropriate network troubleshooting tools.

NEW QUESTION: 109

Which of the following tools uses ICMP to help determine whether a network host is reachable?

A. tcpdump

B. netstat

C. nslookup

D. ping

Answer: D (LEAVE A REPLY)

Ping sends ICMP Echo Request packets and waits for Echo Replies to verify host reachability and measure round-trip time.

A). tcpdump captures packets but does not test reachability.

B). netstat displays open ports and network sessions.

C). nslookup queries DNS servers for name resolution.

References (CompTIA Network+ N10-009):

Domain: Networking Concepts - ICMP operation, troubleshooting tools.

NEW QUESTION: 110

A company security policy requires all network traffic from remote employees' corporate laptops to use the company's VPN. Which of the following network access methods best describes this scenario?

- A. Clientless VPN
- B. Full-tunnel
- C. Site-to-site tunnel
- D. Split-tunnel

Answer: ([SHOW ANSWER](#))

The correct answer is Full-tunnel because the policy requires all network traffic from remote corporate laptops to pass through the company's VPN. In a full-tunnel VPN configuration, once the VPN connection is established, all traffic-including internet-bound traffic-is routed through the corporate network before reaching its destination. This ensures centralized monitoring, content filtering, logging, and enforcement of security controls such as IDS/IPS and firewalls.

According to CompTIA Network+ (N10-009) security objectives, full-tunnel VPNs enhance security by preventing users from directly accessing the internet from their local connection, thereby reducing exposure to local network threats (e.g., public Wi-Fi attacks).

A split-tunnel VPN (Option D) allows users to access the internet directly while only sending corporate-bound traffic through the VPN, which does not meet the "all traffic" requirement. A site-to-site tunnel (Option C) connects entire networks rather than individual remote users. A clientless VPN (Option A) typically provides web-based access without a full network tunnel and does not necessarily route all traffic.

Therefore, full-tunnel best matches the policy requirement.

NEW QUESTION: 111

Which of the following is used to describe the average duration of an outage for a specific service?

- A. RPO
- B. MTTR
- C. RTO
- D. MTBF

Answer: ([SHOW ANSWER](#))

MTTR (Mean Time to Repair) is the average time it takes to repair a system or service after a failure. It helps in measuring the downtime and planning recovery processes.

NEW QUESTION: 112

Which of the following steps of the troubleshooting methodology would most likely involve comparing current throughput tests to a baseline?

- A. Implement the solution
- B. Verify full system functionality
- C. Document findings
- D. Test the theory

Answer: ([SHOW ANSWER](#))

Verifying full system functionality occurs after implementing a fix. This step ensures the solution resolved the issue and that performance is back to expected levels. Comparing current throughput to baseline measurements is part of validation testing to confirm everything is within normal operational parameters.

- A). Implement the solution applies the fix but does not confirm results.
- C). Document findings happens at the end of troubleshooting.
- D). Test the theory comes earlier, when trying to confirm the suspected cause.

References (CompTIA Network+ N10-009):

Domain: Network Troubleshooting - Troubleshooting methodology steps, baselines, verification testing.

NEW QUESTION: 113

Which of the following is a major difference between an IPS and IDS?

- A. An IPS needs to be installed in line with traffic and an IDS does not.
- B. An IPS is signature-based and an IDS is not.
- C. An IPS is less susceptible to false positives than an IDS.
- D. An IPS requires less administrative overhead than an IDS.

Answer: ([SHOW ANSWER](#))

The key difference is that an Intrusion Prevention System (IPS) is installed in line with network traffic, allowing it to actively block threats. In contrast, an Intrusion Detection System (IDS) only monitors and alerts without actively blocking traffic.

Breakdown of Options:

- A). An IPS needs to be installed in line with traffic and an IDS does not. # Correct answer. IPS actively prevents threats, while IDS only detects them.
- B). An IPS is signature-based and an IDS is not. - False, both can use signature-based detection.
- C). An IPS is less susceptible to false positives than an IDS. - False, both can produce false positives, depending on configurations.
- D). An IPS requires less administrative overhead than an IDS. - False, IPS requires more administrative effort due to real-time blocking decisions.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 3.4: Explain network security devices.

NEW QUESTION: 114

Which of the following dynamic routing protocols is used on the internet?

- A. EIGRP
- B. BGP
- C. RIP
- D. OSPF

Answer: ([SHOW ANSWER](#))

BGP (Border Gateway Protocol) is the only dynamic routing protocol used across the internet. It's classified as an Exterior Gateway Protocol (EGP), responsible for routing between different autonomous systems (ASes).

- A). EIGRP and D. OSPF are Interior Gateway Protocols (IGPs), used within organizations.
- C). RIP is an outdated IGP with limited use, unsuitable for internet-scale routing.

Reference:

CompTIA Network+ N10-009 Official Objectives: 3.1 - Compare and contrast various routing technologies.

NEW QUESTION: 115

A network engineer runs ipconfig and notices that the default gateway is 0.0.0.0. Which of the following address types is in use?

- A. APIPA

- B. Multicast
- C. Class C
- D. Experimental

Answer: ([SHOW ANSWER](#))

APIPA (Automatic Private IP Addressing) assigns an IP address in the range 169.254.x.x when a DHCP server cannot be contacted, and it sets the default gateway to 0.0.0.0 because APIPA is designed only for local communication within the same subnet. The document states: "APIPA allows for automatic, ad hoc network communication within a single subnet when a DHCP server is not available. In this state, the default gateway is typically set to 0.0.0.0 because APIPA does not provide routing to other networks."

NEW QUESTION: 116

A technician is troubleshooting a computer issue for a user who works in a new annex of an office building. The user is reporting slow speeds and intermittent connectivity. The computer is connected via a Cat 6 cable to a distribution switch that is 492ft (150m) away. Which of the following should the technician implement to correct the issue?

- A. Increase the bandwidth allocation to the computer.
- B. Install an access switch in the annex and run fiber to the distribution switch.
- C. Run a Cat 7 cable from the computer to the distribution switch.
- D. Enable the computer to support jumbo frames.

Answer: ([SHOW ANSWER](#))

The maximum recommended length for Ethernet cable runs is 100 meters (328 feet). At 150 meters, the Cat 6 cable is too long, causing signal degradation and connectivity issues. Running fiber from the distribution switch to an access switch in the annex will allow for reliable connectivity over longer distances, as fiber can cover greater distances without signal loss. (Reference: CompTIA Network+ Study Guide, Chapter on Network Cable Standards)

NEW QUESTION: 117

Which of the following is the MOST appropriate solution to extend the network to a building located across the street from the main facility?

- A. Multimode fiber
- B. 802.11ac wireless bridge
- C. Cat 6 copper
- D. Loopback adapter

Answer: ([SHOW ANSWER](#))

An 802.11ac wireless bridge is the most practical solution to connect two nearby buildings without trenching or laying physical cable. It provides high-speed, point-to-point connectivity using directional antennas.

- * A. Multimode fiber is effective but expensive and typically limited to 500 meters or less.
- * C. Cat 6 copper is only rated for up to 100 meters - not viable for a street-wide distance.
- * D. Loopback adapter is a troubleshooting tool, not for network extension.

#Reference:

CompTIA Network+ N10-009 Official Objectives: 1.3 - Compare and contrast various network topologies, types, and technologies.

NEW QUESTION: 118

A network technician needs to configure IP addressing in a Class C network with eight subnets total:
Three subnets for 60 hosts

Three subnets for 15 hosts

Two subnets for seven hosts

Which of the following solutions should the technician use to accomplish this task?

A. CIDR

B. APIPA

C. VLSM

D. RFC 1918

Answer: ([SHOW ANSWER](#))

The correct answer is VLSM (Variable Length Subnet Masking). According to the CompTIA Network+ N10-009 objectives, VLSM allows a network administrator to create subnets of different sizes within the same network, making it ideal for environments where subnet host requirements vary.

In this scenario, the technician must support multiple subnet sizes-60 hosts, 15 hosts, and seven hosts- within a single Class C network. Using a single subnet mask for all eight subnets would either waste a large number of IP addresses or fail to meet host requirements. VLSM solves this problem by allowing each subnet to be assigned a custom subnet mask that closely matches its host needs, maximizing address efficiency.

CIDR enables classless addressing and route aggregation but does not, by itself, describe creating multiple subnet sizes within a single address block. APIPA is a self-assigned addressing mechanism used when DHCP fails and has no relevance to subnet design. RFC 1918 defines private IP address ranges but does not address subnetting strategies.

The Network+ objectives emphasize VLSM as a best practice for efficient IP address management, especially in enterprise environments where conserving address space and meeting diverse departmental requirements are critical. In this case, VLSM is the only solution capable of meeting all stated constraints.

NEW QUESTION: 119

Which of the following best describes the purpose of a UPS and PDU in a network installation?

A. To support voltage requirements for devices in an IDF

B. To manage power consumption in the MDF

C. To connect multiple devices to a single network connection

D. To regulate temperature in the MDF and IDF

Answer: ([SHOW ANSWER](#))

The correct answer is A. To support voltage requirements for devices in an IDF. In the CompTIA Network+ N10-009 objectives, network infrastructure includes power systems such as Uninterruptible Power Supplies (UPS) and Power Distribution Units (PDU), which are critical components in both MDF (Main Distribution Frame) and IDF (Intermediate Distribution Frame) environments.

A UPS provides temporary backup power during electrical outages and also conditions power by protecting against surges, spikes, and voltage fluctuations. This ensures that sensitive network equipment such as switches, routers, and servers can continue operating or safely shut down. A PDU, on the other hand, distributes electrical power to multiple devices within a rack, ensuring that all equipment receives the appropriate voltage and sufficient power capacity.

Option B is incorrect because while PDUs can help distribute power, they do not directly manage or optimize power consumption. Option C refers to networking devices like switches, not power equipment. Option D relates to environmental controls such as HVAC systems, not UPS or PDU devices.

Therefore, the primary purpose of UPS and PDU systems is to ensure stable and adequate power delivery to network devices, particularly in environments like IDFs.

NEW QUESTION: 120

A network administrator is connecting two Layer 2 switches in a network. These switches must transfer data in multiple networks. Which of the following would fulfill this requirement?

- A. Jumbo frames
- B. 802.1Q tagging
- C. Native VLAN
- D. Link aggregation

Answer: ([SHOW ANSWER](#))

802.1Q tagging, also known as VLAN tagging, is used to identify VLANs on a trunk link between switches.

This allows the switches to transfer data for multiple VLANs (or networks) over a single physical connection.

This method ensures that traffic from different VLANs is properly separated and managed across the network.

References: CompTIA Network+ study materials.

NEW QUESTION: 121

Which of the following allows a user to authenticate to multiple resources without requiring additional passwords?

- A. SSO
- B. MFA
- C. SAML
- D. RADIUS

Answer: ([SHOW ANSWER](#))

The correct answer is SSO (Single Sign-On) because it enables a user to authenticate once and gain access to multiple systems or resources without being prompted to log in again. According to CompTIA Network+ (N10-009) security objectives, SSO improves usability and productivity while maintaining centralized authentication control. After the initial authentication, a trust relationship between systems allows the user to access additional applications seamlessly.

MFA (Multi-Factor Authentication) enhances security by requiring two or more authentication factors (something you know, have, or are), but it does not inherently provide access to multiple systems without repeated authentication events.

SAML (Security Assertion Markup Language) is an authentication and authorization protocol commonly used to implement SSO in web-based environments. While SAML supports SSO functionality, it is the underlying protocol rather than the access method itself.

RADIUS is a centralized authentication, authorization, and accounting (AAA) protocol used for network access control but does not specifically provide seamless multi-resource authentication without additional logins.

Therefore, SSO best describes authentication to multiple resources without requiring additional passwords.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here: <https://www.edudump.com/exams/CompTIA/N10-009/premium/> (608 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 122

Which of the following is the most likely reason an insurance brokerage would enforce VPN usage?

- A. To encrypt sensitive data in transit
- B. To secure the endpoint
- C. To maintain contractual agreements
- D. To comply with data retention requirements

Answer: ([SHOW ANSWER](#))

The most likely reason an insurance brokerage would enforce VPN usage is to encrypt sensitive data in transit. VPNs (Virtual Private Networks) create a secure tunnel between the user's device and the corporate network, ensuring that data is encrypted and protected from interception.

* Encryption: VPNs encrypt data, preventing unauthorized access and ensuring data privacy during transmission over public or unsecured networks.

* Data Protection: Essential for industries handling sensitive information, such as insurance brokerages, to protect customer data and comply with regulatory requirements.

* Security: Enhances overall network security by providing secure remote access for employees.

Network References:

* CompTIA Network+ N10-007 Official Certification Guide: Discusses the role of VPNs in securing data in transit.

* Cisco Networking Academy: Provides training on VPN technologies and their importance in data security.

* Network+ Certification All-in-One Exam Guide: Explains VPN usage and its benefits in protecting sensitive information.

NEW QUESTION: 123

A company is implementing a disaster recovery plan in case of a network security incident. Which of the following steps must be included in the disaster recovery plan?

- A. Schedule network vulnerability scans
- B. Install antivirus software on all devices
- C. Back up all data regularly
- D. Deploy an IDS on all networks

Answer: ([SHOW ANSWER](#))

Regularly backing up all data is a required part of a disaster recovery plan. Disaster recovery focuses on restoring systems, services, data, and business operations after a disruptive event such as ransomware, data corruption, hardware failure, natural disaster, or a major network security incident. Without reliable backups, an organization may be unable to recover lost or encrypted data, rebuild critical systems, or meet recovery time and recovery point objectives.

The CompTIA Network+ N10-009 objectives include disaster recovery, business continuity, backups, recovery planning, and operational resilience. A proper DR plan should include backup frequency, backup location, retention policy, restoration testing, access control, encryption, and procedures for recovering critical network services.

Vulnerability scans are useful for identifying weaknesses before an incident occurs, but they are part of risk management and security assessment rather than the core recovery process. Antivirus software helps prevent or detect malware, but it does not guarantee recovery after an incident. An IDS can detect suspicious activity, but it does not restore data or services. Therefore, regular data backups are the required disaster recovery step.

NEW QUESTION: 124

Which of the following is used to estimate the average life span of a device?

- A. RTO
- B. RPO

C. MTBF

D. MTTR

Answer: ([SHOW ANSWER](#))

* Understanding MTBF:

* Mean Time Between Failures (MTBF): A reliability metric that estimates the average time between successive failures of a device or system.

* Calculation and Importance:

* Calculation: MTBF is calculated as the total operational time divided by the number of failures during that period.

* Usage: Used by manufacturers and engineers to predict the lifespan and reliability of a device, helping in maintenance planning and lifecycle management.

* Comparison with Other Metrics:

* RTO (Recovery Time Objective): The maximum acceptable time to restore a system after a failure.

* RPO (Recovery Point Objective): The maximum acceptable amount of data loss measured in time.

* MTTR (Mean Time to Repair): The average time required to repair a device or system and return it to operational status.

* Application:

* MTBF is crucial for planning maintenance schedules, spare parts inventory, and improving the overall reliability of systems.

References:

* CompTIA Network+ study materials on reliability and maintenance metrics.

NEW QUESTION: 125

A network administrator needs to set up a multicast network for audio and video broadcasting. Which of the following networks would be the most appropriate for this application?

A. 172.16.0.0/24

B. 192.168.0.0/24

C. 224.0.0.0/24

D. 240.0.0.0/24

Answer: ([SHOW ANSWER](#))

* Understanding Multicast:

* Multicast IP Address Range: The multicast address range is from 224.0.0.0 to 239.255.255.255, designated for multicast traffic.

* Multicast Applications:

* Use Case: Multicast is used for one-to-many or many-to-many communication, suitable for applications like audio and video broadcasting where the same data is sent to multiple recipients simultaneously.

* Appropriate Network Selection:

* 224.0.0.0/24 Network: This range is reserved for multicast addresses, making it the appropriate choice for setting up a multicast network.

* Comparison with Other Options:

* 172.16.0.0/24: Part of the private IP address space, used for private networks, not designated for multicast.

* 192.168.0.0/24: Another private IP address range, also not for multicast.

* 240.0.0.0/24: Reserved for future use, not suitable for multicast.

References:

* CompTIA Network+ study materials on IP address ranges and multicast.

NEW QUESTION: 126

An organization requires the ability to send encrypted email messages to a partner from an email server that is hosted on premises. The organization prefers to use the standard default ports when creating firewall rules.

Which of the following ports should be open to satisfy the requirements?

- A. 110
- B. 143
- C. 587
- D. 636

Answer: ([SHOW ANSWER](#))

Port 587 is the standard default port for sending email (SMTP) with TLS encryption, which is used to secure email transmissions between mail servers or between clients and mail servers. Allowing traffic over port 587 enables secure email sending while maintaining standard protocol usage. (Reference: CompTIA Network+ Study Guide, Chapter on Ports and Protocols)

NEW QUESTION: 127

Which of the following would an adversary do while conducting an evil twin attack?

- A. Trick users into using an AP with an SSID that is identical to a legitimate network
- B. Manipulate address resolution to point devices to a malicious endpoint
- C. Present an identical MAC to gain unauthorized access to network resources
- D. Capture data in transit between two legitimate endpoints to steal data

Answer: ([SHOW ANSWER](#))

An evil twin attack sets up a rogue AP with the same SSID as a legitimate wireless network, tricking users into connecting. Once connected, the attacker can intercept traffic or harvest credentials.

B). Describes ARP spoofing.

C). Describes MAC spoofing.

D). Describes on-path attacks, which may follow, but the evil twin method begins with SSID impersonation.

References (CompTIA Network+ N10-009):

Domain: Network Security - Wireless threats, rogue APs, evil twin.

NEW QUESTION: 128

Which of the following connector types would most likely be used to connect to an external antenna?

- A. BNC
- B. ST
- C. LC
- D. MPO

Answer: ([SHOW ANSWER](#))

BNC connectors are commonly used for coaxial cables, including those connecting to external antennas in Wi-Fi, radio, and surveillance systems.

Breakdown of Options:

A). BNC - Correct answer. Used for coaxial cables in wireless and antenna connections.

B). ST - Used for fiber optic cables, not antennas.

C). LC - A fiber optic connector, not for antennas.

D). MPO - Used for multi-fiber optic cables, not RF antennas.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 1.1: Compare and contrast physical network connectors.

IEEE 802.11: Wireless standards and antenna connectors

NEW QUESTION: 129

A company's VoIP phone connection is cutting in and out. A senior network engineer is recommending the implementation of a voice VLAN. Which of the following should be configured?

- A. 802.1Q tagging
- B. Jumbo frames
- C. Native VLAN
- D. Link aggregation

Answer: ([SHOW ANSWER](#))

Voice VLANs rely on 802.1Q tagging to separate voice traffic from data traffic on the same physical link.

This separation allows QoS policies to prioritize VoIP, reducing jitter and packet loss.

- B). Jumbo frames improve throughput for large data transfers, not voice.
- C). Native VLAN is the untagged VLAN, not specifically for voice.
- D). Link aggregation bundles links for bandwidth/redundancy, not QoS.

References (CompTIA Network+ N10-009):

Domain: Network Infrastructure - VLANs, voice VLANs, 802.1Q tagging, QoS.

NEW QUESTION: 130

A network administrator deploys new network hardware. While configuring the network monitoring server, the server could not authenticate but could not determine the specific status of the hardware. Which of the following would the administrator most likely do to resolve the issue?

- A. Use the public community string
- B. Import the appropriate MIB
- C. Set up a switchport analyzer and forward traffic
- D. Configure SNMPv3 privacy

Answer: ([SHOW ANSWER](#))

MIBs (Management Information Bases) define the variables and objects that SNMP can query on a device. If the monitoring server authenticates but cannot interpret the data, it likely lacks the correct MIB for that vendor or model. Importing the proper MIB allows the monitoring server to correctly display device status and metrics.

- A). Using a public community string is insecure and not related to missing MIBs.
- C). Switchport analyzer (SPAN) captures traffic for packet analysis, not SNMP monitoring.
- D). SNMPv3 privacy adds encryption but doesn't fix missing MIB interpretation.

References (CompTIA Network+ N10-009):

Domain: Network Operations - SNMP, MIBs, network monitoring systems.

NEW QUESTION: 131

Which of the following steps of the troubleshooting methodology comes after testing the theory to determine cause?

- A. Verify full system functionality.

- B. Document the findings and outcomes.
- C. Establish a plan of action.
- D. Identify the problem.

Answer: (SHOW ANSWER)

The CompTIA Troubleshooting Methodology states that after testing the theory, the next step is to establish a plan of action to resolve the issue.

Troubleshooting Steps:

Identify the problem.

Establish a theory of probable cause.

Test the theory to determine the cause.

Establish a plan of action and implement the solution. # (Correct step) Verify full system functionality.

Document findings, actions, and outcomes.

Breakdown of Options:

A: Verify full system functionality - Happens after implementing the solution.

B: Document the findings and outcomes - Final step, happens after resolving the issue.

C: Establish a plan of action - # Correct answer. Comes immediately after confirming the cause.

D: Identify the problem - First step, already completed.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 5.1: Explain network troubleshooting methodology.

NEW QUESTION: 132

A technician is designing a cloud service solution that will accommodate the company's current size, compute capacity, and storage capacity.

Which of the following cloud deployment models will fulfill these requirements?

- A. SaaS
- B. PaaS
- C. IaaS
- D. IaC

Answer: (SHOW ANSWER)

Infrastructure as a Service (IaaS) provides scalable compute power, storage, and networking resources on demand. It is the best choice for a company that needs to customize its cloud solution based on size, compute capacity, and storage needs.

IaaS Benefits:

Provides virtual machines, storage, and networking resources.

Scalable based on company needs.

Reduces the need for physical infrastructure.

Incorrect Options:

A: SaaS (Software as a Service): Delivers software applications (e.g., Google Docs, Microsoft 365) but does not provide compute/storage infrastructure.

B: PaaS (Platform as a Service): Provides a development environment for application deployment but not full infrastructure control.

D: IaC (Infrastructure as Code): A methodology for automating infrastructure, not a cloud deployment model.

Reference:

CompTIA Network+ N10-009 Official Study Guide - Chapter on Cloud Computing Models

NEW QUESTION: 133

Which of the following steps in the troubleshooting methodology includes checking logs for recent changes?

- A. Identify the problem.
- B. Document the findings and outcomes.
- C. Test the theory to determine cause.
- D. Establish a plan of action.

Answer: ([SHOW ANSWER](#))

Reference: CompTIA Network+ Certification Exam Objectives - Troubleshooting section.

NEW QUESTION: 134

A firewall receives traffic on port 80 and forwards it to an internal server on port 88. Which of the following technologies is being leveraged?

- A. TLS
- B. FHRP
- C. SSL
- D. PAT

Answer: ([SHOW ANSWER](#))

The correct answer is PAT (Port Address Translation). According to the CompTIA Network+ N10-009 objectives, PAT is a form of Network Address Translation (NAT) that allows multiple internal hosts-or services-to be mapped to a single public IP address using different port numbers. PAT can also translate destination port numbers, which is exactly what is occurring in this scenario.

In this case, the firewall receives incoming traffic on port 80 (commonly used for HTTP) and forwards it to an internal server listening on port 88. This process is often referred to as port forwarding, which is a practical implementation of PAT. The firewall rewrites the destination port and potentially the destination IP address so that external clients can access internal services without exposing internal addressing schemes. The other options do not apply. TLS and SSL are encryption protocols used to secure data in transit; they do not perform port translation. FHRP (First Hop Redundancy Protocol), such as HSRP or VRRP, provides gateway redundancy and high availability, not traffic forwarding or port remapping.

The Network+ objectives emphasize understanding how firewalls and NAT technologies manipulate IP addresses and ports to enable secure access to internal resources. PAT is the technology that enables this functionality, making it the correct answer.

NEW QUESTION: 135

Which of the following is most commonly associated with many systems sharing one IP address in the public IP-addressing space?

- A. PAT
- B. NAT
- C. VIP
- D. NAT64

Answer: ([SHOW ANSWER](#))

Port Address Translation (PAT) allows multiple internal devices to share a single public IP address by assigning each device a unique port number. This is the most common method used in environments where many systems need internet access but there are limited public IP addresses.

NEW QUESTION: 136

A network engineer is designing an internal network that needs to support both IPv4 and IPv6 routing. Which of the following routing protocols is capable of supporting both IPv4 and IPv6?

- A. OSPFv3
- B. RIPv2
- C. BGP
- D. EIGRP

Answer: ([SHOW ANSWER](#))

EIGRP(Enhanced Interior Gateway Routing Protocol) supports both IPv4 and IPv6. While OSPFv3 is specific to IPv6 and RIPv2 only supports IPv4, EIGRP was extended to handle dual-stack environments efficiently.

Reference: Section 2.1 - Characteristics of Routing Technologies - "EIGRP"

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here: <https://www.edudump.com/exams/CompTIA/N10-009/premium/> (608 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 137

A network technician is troubleshooting a faulty NIC and tests the theory. Which of the following should the technician do next?

- A. Develop a theory.
- B. Establish a plan of action.
- C. Implement the solution.
- D. Document the findings.

Answer: ([SHOW ANSWER](#))

Once the theory has been tested and confirmed, the next step is to implement the solution based on the CompTIA troubleshooting model.

CompTIA Troubleshooting Model:

Identify the problem.

Establish a theory of probable cause.

Test the theory.

Establish a plan of action and implement the solution. # (Correct step) Verify full system functionality.

Document findings, actions, and outcomes.

Breakdown of Options:

- A). Develop a theory - The theory has already been developed and tested.
- B). Establish a plan of action - This happens before implementation, but since the issue is confirmed, it's time to act.
- C). Implement the solution - Correct answer. The problem is confirmed, so the fix should be applied.
- D). Document the findings - Documentation is the final step, not the next one.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 5.1: Explain network troubleshooting methodology.

NEW QUESTION: 138

Users are reporting issues with mobile phone connectivity after a cellular repeater was recently installed.

Users also note that the phones are rapidly losing battery charge. Which of the following should the technician check first to troubleshoot the issue?

- A. WPS configuration
- B. Signal strength
- C. Channel frequency
- D. Power budget

Answer: (SHOW ANSWER)

When signal strength is poor, mobile devices constantly boost their transmission power in an attempt to maintain a stable connection. This results in dropped calls/data and rapid battery drain. Since a repeater was installed, misalignment or misconfiguration could be degrading the signal strength.

A). WPS applies to Wi-Fi, not cellular repeaters.

C). Channel frequency might matter for interference, but signal strength is the most direct cause of the described symptoms.

D). Power budget applies to PoE and wired devices, not mobile phones.

References (CompTIA Network+ N10-009):

Domain: Network Troubleshooting - Wireless/cellular troubleshooting, signal strength impact, user symptoms (battery drain, poor connectivity).

NEW QUESTION: 139

A network administrator prepares a VLAN for a new office while planning for minimal IP address waste. The new office will have approximately 800 workstations. Which of the following network schemes meets the requirements?

- A. 10.0.100.0/22
- B. 172.16.8.0/23
- C. 172.16.15.0/20
- D. 192.168.4.0/21

Answer: (SHOW ANSWER)

To support about 800 workstations with minimal IP waste, you choose the smallest subnet that provides at least 800 usable host addresses. In IPv4, usable hosts per subnet are calculated as $2^{(\text{host bits})} \# 2$ (subtracting network and broadcast addresses). A /22 leaves 10 host bits ($32 \# 22 = 10$), providing $2^{10} \# 2 =$

$1024 \# 2 = 1022$ usable addresses-enough for 800 devices with relatively low waste.

Check the other options: /23 leaves 9 host bits, giving $2^9 \# 2 = 512 \# 2 = 510$ usable addresses, which is not enough. A /21 provides $2^{11} \# 2 = 2048 \# 2 = 2046$ usable addresses-enough, but wastes more than /22. A

/20 provides $2^{12} \# 2 = 4096 \# 2 = 4094$ usable addresses-much more waste.

Therefore, 10.0.100.0/22 is the best choice that meets the workstation requirement while minimizing unused addresses.

NEW QUESTION: 140

An investment bank is seeking a DR backup solution. Which of the following provides the most cost-effective backup site?

- A. Hot
- B. Cold
- C. Cluster
- D. Warm

Answer: ([SHOW ANSWER](#))

*Cold sites are the most cost-effective disaster recovery (DR) option since they require the least infrastructure investment. They provide space and power but no pre-configured systems.

*Hot sites (A) are fully operational and very expensive.

*Warm sites (D) offer some pre-configured hardware but still require setup, making them more costly than cold sites.

*Clusters (C) are active failover systems, not DR sites.

#Reference: CompTIA Network+ N10-009 Official Documentation - Disaster Recovery & Business Continuity Planning.

NEW QUESTION: 141

While troubleshooting a VoIP handset connection, a technician's laptop is able to successfully connect to network resources using the same port. The technician needs to identify the port on the switch. Which of the following should the technician use to determine the switch and port?

A. LLDP

B. IKE

C. VLAN

D. netstat

Answer: ([SHOW ANSWER](#))

Link Layer Discovery Protocol (LLDP) is a network protocol used for discovering devices and their capabilities on a local area network, primarily at the data link layer (Layer 2). It helps in identifying the connected switch and the specific port to which a device is connected. When troubleshooting a VoIP handset connection, the technician can use LLDP to determine the exact switch and port where the handset is connected. This protocol is widely used in network management to facilitate the discovery of network topology and simplify troubleshooting.

Other options such as IKE (Internet Key Exchange), VLAN (Virtual LAN), and netstat (network statistics) are not suitable for identifying the switch and port information. IKE is used in setting up secure IPsec connections, VLAN is used for segmenting networks, and netstat provides information about active connections and listening ports on a host but not for discovering switch port details.

Reference: CompTIA Network+ Certification Exam Objectives - Network Troubleshooting and Tools section.

NEW QUESTION: 142

Users report performance issues on the network. A network administrator notices broadcast storms occurring.

Which of the following protocols should the administrator configure to mitigate this issue?

A. Spanning Tree

B. Enhanced Interior Gateway Routing Protocol (EIGRP)

C. Cisco Discovery Protocol (CDP)

D. Link Layer Discovery Protocol (LLDP)

E. Border Gateway Protocol (BGP)

Answer: ([SHOW ANSWER](#))

The correct answer is Spanning Tree because broadcast storms are typically caused by Layer 2 switching loops in Ethernet networks. According to the CompTIA Network+ (N10-009) objectives under switching concepts, the Spanning Tree Protocol (STP) is specifically designed to prevent loops in networks that have redundant switch connections.

In a Layer 2 environment, switches forward broadcast frames out all ports except the one on which they were received. If redundant paths exist without STP, frames can circulate indefinitely, creating a broadcast storm.

This results in excessive traffic, high CPU utilization on switches, MAC address table instability, and significant network performance degradation.

STP prevents this by logically blocking redundant paths while maintaining them as backups. If the active path fails, STP recalculates and activates a previously blocked path, preserving redundancy without loops.

The other options-EIGRP and BGP (routing protocols) and CDP and LLDP (device discovery protocols)- do not prevent Layer 2 loops.

Therefore, configuring Spanning Tree Protocol is the appropriate solution to mitigate broadcast storms.

NEW QUESTION: 143

A network engineer needs to order cabling to connect two buildings within the same city. Which of the following media types should the network engineer use?

- A.** Coaxial
- B.** Twinaxial
- C.** Single-mode fiber
- D.** Cat 5

Answer: C ([LEAVE A REPLY](#))

Single-mode fiber is best suited for long-distance communication, often exceeding 10 km (6.2 miles). It's immune to EMI and offers high bandwidth - making it the ideal choice for connecting buildings across a city.

Coaxial (A) and Twinaxial (B) are used for shorter distances and specific use cases (e.g., storage or legacy systems).

Cat 5 (D) is limited to 100 meters and is not suitable for city-level interconnects.

For long-distance, high-speed, and reliable communication between buildings, Single-mode fiber is the professional choice.

Reference:CompTIA Network+ N10-009 Official Study Guide - Objective 3.4: "Summarize the properties and purposes of physical network topologies and network types."

NEW QUESTION: 144

Which of the following requires network devices to be managed using a different set of IP addresses?

- A.** Console
- B.** Split tunnel
- C.** Jump box
- D.** Out of band

Answer: ([SHOW ANSWER](#)**)**

Out-of-band (OOB) management refers to using a dedicated management network that is physically separate from the regular data network. This management network uses a different set of IP addresses to ensure that management traffic is isolated from user data traffic, providing a secure way to manage network devices even if the main network is down or compromised.References:CompTIA Network+ study materials.

NEW QUESTION: 145

Which of the following ports is a secure protocol?

- A.** 20
- B.** 23
- C.** 443
- D.** 445

Answer: ([SHOW ANSWER](#)**)**

Port 443 is used by HTTPS (Hypertext Transfer Protocol Secure), a secure version of HTTP that uses SSL

/TLS to encrypt the communication between a client and server. This ensures confidentiality and integrity of data in transit. The document states:

"Port 443 is the default port for HTTPS, which secures HTTP traffic using SSL/TLS, providing encryption and secure identification of web servers."

NEW QUESTION: 146

Ten new laptops are added to an existing network, and they can only communicate with one another. An administrator reviews documentation and sees the following:

Subnet: 10.8.100.1/24

Scope: 10.8.100.50 - 10.8.100.150

Reservation: 10.8.100.151 - 10.8.100.175

A technician scans the network and receives the following results:

IP addresses used: 10.8.100.45 - 10.8.100.175

Which of the following should be done to ensure connectivity on all laptops?

A. Increase the scope to 10.8.100.35 - 10.8.100.150

B. Increase the scope to 10.8.100.40 - 10.8.100.150

C. Increase the scope to 10.8.100.40 - 10.8.100.175

D. Increase the scope to 10.8.100.50 - 10.8.100.175

Answer: (SHOW ANSWER)

The correct answer is D: Increase the scope to 10.8.100.50 - 10.8.100.175. According to the CompTIA Network+ N10-009 objectives, proper DHCP scope configuration is essential to ensure all hosts can obtain valid IP addresses and communicate beyond their local segment.

In this scenario, the DHCP scope is configured for 10.8.100.50 through 10.8.100.150, while a reservation range exists from 10.8.100.151 through 10.8.100.175. The network scan shows that IP addresses up to

10.8.100.175 are already in use. This indicates that some devices are either statically assigned addresses outside the active scope or are failing to receive valid DHCP leases, causing the new laptops to communicate only with each other-often a sign of APIPA or improper addressing.

To ensure full connectivity, the DHCP scope must be expanded to include the entire range of addresses that are actively in use, including the reserved addresses. Option D correctly extends the scope to 10.8.100.175 without overlapping lower addresses that may be statically assigned or intentionally excluded.

The Network+ objectives emphasize avoiding address conflicts and ensuring DHCP scopes align with real-world network usage. Expanding the scope to include all valid addresses ensures that all laptops can obtain proper IP configuration, default gateway information, and full network connectivity.

NEW QUESTION: 147

A network administrator is reviewing a production web server and observes the following output from the netstat command:

Which of the following actions should the network administrator take to harden the security of the web server?

A. Disable the unused ports.

B. Enforce access control lists.

C. Perform content filtering.

D. Set up a screened subnet.

Answer: A (LEAVE A REPLY)

The netstat output shows that multiple ports are open, including Telnet (23), FTP (20), and TFTP (69), which are potential security risks. Disabling unused ports minimizes the attack surface, reducing security vulnerabilities.

Breakdown of Options:

A). Disable the unused ports - Correct answer. Unused ports should be closed to prevent unauthorized access.

- B). Enforce access control lists - ACLs help control access but do not disable unnecessary services.
- C). Perform content filtering - Content filtering controls web traffic, not port security.
- D). Set up a screened subnet - A DMZ (screened subnet) improves security but does not address open ports.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 3.4: Given a scenario, implement network security measures.

CIS Benchmark for Linux & Windows Server Hardening

NEW QUESTION: 148

Which of the following is most likely affected when executing a successful DoS attack?

- A. Bandwidth
- B. NAT pool
- C. ACL
- D. Storage availability

Answer: A ([LEAVE A REPLY](#))

Bandwidth is most likely affected during a successful denial-of-service attack. A DoS attack attempts to make a system, service, or network unavailable to legitimate users. One common method is flooding the target with excessive traffic, which consumes bandwidth, processing resources, or connection capacity. When bandwidth is overwhelmed, legitimate users may experience slow connections, dropped sessions, failed requests, or complete service unavailability.

The CompTIA Network+ N10-009 objectives include identifying common attacks and understanding their effect on network availability. DoS and DDoS attacks primarily target availability, one of the three core security goals in the CIA triad: confidentiality, integrity, and availability. Network-based DoS attacks often generate large amounts of traffic, making bandwidth a primary resource under attack.

A NAT pool could be exhausted in certain attack scenarios, but it is not the most general or most likely answer. An ACL is a rule set used to permit or deny traffic; it may help mitigate an attack but is not usually the resource being consumed. Storage availability could be affected in some application-specific attacks, but bandwidth is the best answer for a typical DoS attack.

NEW QUESTION: 149

Which of the following would most likely be used as a replacement for a traditional VPN for remote users?

- A. SD-WAN
- B. SASE
- C. Site-to-site VPN
- D. Reverse proxy

Answer: ([SHOW ANSWER](#)**)**

A modern replacement for traditional remote-access VPN for users is SASE (Secure Access Service Edge).

Network+ highlights trends in remote connectivity and security where organizations move away from backhauling all user traffic through a VPN concentrator and instead use cloud-delivered security and access controls closer to the user. SASE combines networking and security capabilities-commonly including ZTNA (Zero Trust Network Access), secure web gateway (SWG), CASB, firewall-as-a-service (FWaaS), and centralized policy enforcement-so remote users can securely access applications without relying on a classic "connect to the corporate network first" VPN model.

SD-WAN primarily optimizes connectivity between sites and to cloud services, often for branch networks; it's not typically the direct replacement for remote user VPN access. Site-to-site VPN connects networks (locations) and is not intended for individual remote users. A reverse proxy can publish specific internal web applications externally and provide some security functions, but it does not replace VPN broadly for remote user

access to multiple internal resources the way SASE/Zero Trust access solutions do. Therefore, SASE is the best answer as the likely replacement for traditional remote-access VPN.

NEW QUESTION: 150

A company's network is experiencing high levels of suspicious network traffic. The security team finds that the traffic is coming from an unknown, foreign IP address. Which of the following is the most cost-efficient way to mitigate this threat?

- A. ACL
- B. IDS
- C. NAT
- D. DoS prevention

Answer: ([SHOW ANSWER](#))

The correct answer is ACL (Access Control List). According to the CompTIA Network+ N10-009 objectives, ACLs are a fundamental and cost-effective method for controlling traffic flow at routers and firewalls. An ACL allows administrators to permit or deny traffic based on source IP address, destination IP address, protocol, or port number.

In this scenario, the suspicious traffic is identified as originating from a specific unknown foreign IP address.

The most direct and economical mitigation strategy is to configure an ACL rule that denies traffic from that specific IP address (or subnet) at the network perimeter. This approach leverages existing network infrastructure without requiring additional hardware or licensing costs.

An IDS (Intrusion Detection System) monitors and alerts on malicious activity but does not actively block traffic unless paired with IPS functionality, and it may involve additional cost and complexity. NAT is used for address translation and does not provide traffic filtering based on threat intelligence. DoS prevention solutions are typically more advanced, specialized, and costly, often intended for large-scale distributed denial-of-service attacks rather than blocking traffic from a single suspicious IP.

The Network+ objectives emphasize implementing layered security controls, starting with simple and effective measures. In this case, applying an ACL at the firewall or router is the most cost-efficient and immediate method to mitigate the identified threat.

NEW QUESTION: 151

Which of the following can also provide a security feature when implemented?

- A. NAT
- B. BGP
- C. FHRP
- D. EIGRP

Answer: ([SHOW ANSWER](#))

NAT (Network Address Translation) helps hide internal IP addresses from external networks, adding a layer of security by preventing direct access to internal systems from the outside.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com

NEW QUESTION: 152

An organization is struggling to get effective coverage using the wireless network. The organization wants to implement a solution that allows for continuous connectivity anywhere in the facility. Which of the following should the network administrator suggest to ensure the best coverage?

- A. Implementing additional ad hoc access points
- B. Providing more Ethernet drops for user connections
- C. Deploying a mesh network in the building
- D. Changing the current frequency of the Wi-Fi

Answer: ([SHOW ANSWER](#))

The correct answer is deploying a mesh network. A mesh wireless network uses multiple interconnected access points that automatically route traffic through the best available path. This ensures seamless coverage throughout a facility, even when users move between APs. Mesh APs can extend coverage without requiring each AP to be directly wired, making them ideal for large or hard-to-wire environments.

- A). Ad hoc access points are peer-to-peer connections and cannot provide enterprise-grade continuous coverage.
- B). Ethernet drops provide wired connectivity but do not solve wireless coverage issues.
- D). Changing the frequency (from 2.4 GHz to 5 GHz or vice versa) may reduce interference but will not guarantee building-wide seamless connectivity.

Mesh networks are particularly effective in environments with roaming devices (smartphones, tablets, handheld scanners) and ensure that there are no dead spots, thereby delivering continuous wireless access.

References (CompTIA Network+ N10-009):

Domain: Network Infrastructure - Wireless architectures, mesh networking, seamless connectivity.

NEW QUESTION: 153

An organization recently connected a new computer to the LAN. The user is unable to ping the default gateway. The technician examines the configuration and sees a self-assigned IP address. Which of the following is the most likely cause?

- A. The DHCP server is not available
- B. An RFC1918 address is being used
- C. The TCP/IP stack is disabled
- D. A static IP is assigned

Answer: A ([LEAVE A REPLY](#))

When a host fails to obtain an IP address from a DHCP server, it assigns itself an APIPA (Automatic Private IP Addressing) address in the 169.254.x.x range, commonly described as a "self-assigned IP." This prevents communication outside the local link, including reaching the default gateway.

- B). RFC1918 addresses are private ranges (10.x.x.x, 172.16-31.x.x, 192.168.x.x), but these are not self-assigned.
- C). If the TCP/IP stack were disabled, the host wouldn't have any IP at all.
- D). If a static IP were assigned, it would show a configured value, not self-assigned.

References (CompTIA Network+ N10-009):

Domain: Network Troubleshooting - IP addressing issues, DHCP failures, APIPA behavior.

NEW QUESTION: 154

A network administrator upgrades the wireless access points and wants to implement a configuration that gives users higher speed and less channel overlap based on device compatibility. Which of the following accomplishes this goal?

- A. 802.1X
- B. MIMO
- C. ESSID
- D. Band steering

Answer: ([SHOW ANSWER](#))

The best solution here is band steering. Band steering allows modern wireless access points to automatically direct dual-band capable clients toward the 5 GHz band instead of the crowded 2.4 GHz band. The 5 GHz band has more available non-overlapping channels and can provide faster speeds with less interference, especially in dense environments. Devices that only support 2.4 GHz will remain on that band, while compatible devices enjoy the improved performance of 5 GHz.

A). 802.1X is a port-based network access control method for authentication. While important for security, it does not affect wireless channel utilization or client throughput.

B). MIMO (Multiple Input, Multiple Output) is a technology that improves throughput by using multiple antennas to send/receive simultaneously, but it does not actively steer clients between frequency bands.

C). ESSID (Extended Service Set Identifier) is just the network name for a set of APs in the same WLAN; it has no role in optimizing performance by band.

By implementing band steering, administrators reduce channel overlap on the 2.4 GHz band, improve spectral efficiency, and provide higher performance to capable devices, directly meeting the requirements described in the scenario.

References (CompTIA Network+ N10-009):

Domain: Networking Concepts - Wireless optimization, band steering, dual-band client management.

NEW QUESTION: 155

A technician is troubleshooting a user's laptop that is unable to connect to a corporate server. The technician thinks the issue pertains to routing. Which of the following commands should the technician use to identify the issue?

- A. tcpdump
- B. dig
- C. tracer
- D. arp

Answer: ([SHOW ANSWER](#))

The tracer (Traceroute) command is used to determine the path packets take from the source to the destination. It helps in identifying routing issues by showing each hop the packets pass through, along with the time taken for each hop. This command can pinpoint where the connection is failing or experiencing delays, making it an essential tool for troubleshooting routing issues. References: CompTIA Network+ study materials and common network troubleshooting commands.

NEW QUESTION: 156

A user is unable to navigate to a website because the provided URL is not resolving to the correct IP address.

Other users are able to navigate to the intended website without issue. Which of the following is most likely causing this issue?

- A. Hosts file
- B. Self-signed certificate
- C. Nameserver record

D. IP helper ANS

Answer: ([SHOW ANSWER](#))

* Role of the Hosts File:

* The hosts file is a local file on a computer that maps hostnames to IP addresses. It can be used to override DNS resolution by providing a static mapping of a hostname to an IP address.

* Common Issues with the Hosts File:

* If an incorrect IP address is mapped to a hostname in the hosts file, it can cause the computer to resolve the hostname to the wrong IP address. This can lead to navigation issues for specific websites while other users, relying on DNS, do not face the same problem.

* Why Other Options are Less Likely:

* Self-signed certificate:Relates to SSL/TLS and would cause a security warning, not a navigation failure.

* Nameserver record:Affects all users, not just one.

* IP helper:Used to forward DHCP requests and is unrelated to DNS resolution issues.

* Troubleshooting Steps:

* Check the hosts file on the affected user's computer (C:\Windows\System32\drivers\etc\hostson Windows or/etc/hostson Unix/Linux).

* Look for entries that map the problematic hostname to an incorrect IP address and correct or remove them.

References:

* CompTIA Network+ study materials and system administration documentation.

NEW QUESTION: 157

A cloud administrator must ensure that all access to social media websites is prohibited. Which of the following should the administrator use to prevent users from accessing those websites?

A. NAC

B. Screened subnet

C. VPN

D. Content filter

Answer: ([SHOW ANSWER](#))

A content filter is the correct solution because it can block access to specific categories of websites, domains, URLs, or application types, including social media. Content filtering is commonly used to enforce acceptable use policies, reduce risk, improve productivity, and prevent users from accessing prohibited or unsafe web content. In this scenario, the requirement is to stop access to social media websites, so filtering web content by category or URL is the most direct control.

The CompTIA Network+ N10-009 objectives include network security concepts, access control, filtering, and security appliances or services. A content filter may be implemented through a secure web gateway, firewall, DNS filtering platform, proxy server, cloud security platform, or endpoint security solution.

Network Access Control, or NAC, controls whether devices are allowed to connect to the network based on identity, posture, or policy. A screened subnet, also called a DMZ, is used to isolate public-facing services. A VPN provides encrypted connectivity but does not inherently block social media access. Therefore, content filtering is the most appropriate answer.

NEW QUESTION: 158

A network technician needs to connect a new user to the company's Wi-Fi network called SSID: business.

When attempting to connect, two networks are listed as possible choices: SSID: business and SSID:

myaccess. Which of the following attacks is occurring?

- A. On-path
- B. Rogue AP
- C. Evil twin
- D. Tailgating

Answer: ([SHOW ANSWER](#))

An evil twin attack occurs when an attacker creates a fraudulent AP with an SSID very similar (or identical) to the legitimate one. Users may accidentally connect, allowing the attacker to capture traffic and credentials.

- A). On-path is the consequence of connecting to the evil twin, not the initial attack itself.
- B). Rogue AP is any unauthorized access point, but the key here is the malicious mimicry of a legitimate SSID - specifically an evil twin.
- D). Tailgating is a physical social engineering attack, unrelated to Wi-Fi.

References (CompTIA Network+ N10-009):

Domain: Network Security - Wireless threats (rogue APs, evil twins).

NEW QUESTION: 159

Which of the following will allow secure, remote access to internal applications?

- A. VPN
- B. CDN
- C. SAN
- D. IDS

Answer: ([SHOW ANSWER](#))

A Virtual Private Network (VPN) creates an encrypted connection between a remote user and an internal network, ensuring secure access to internal applications.

- * VPNs use encryption protocols like IPSec and SSL/TLS to protect data during transmission.
 - * They are widely used for secure remote work, accessing company resources, and bypassing geographic restrictions.
 - * Option B (CDN - Content Delivery Network): Used for speeding up website content delivery, not for remote access security.
 - * Option C (SAN - Storage Area Network): Used for high-speed storage, unrelated to remote access.
 - * Option D (IDS - Intrusion Detection System): Monitors for malicious activities but does not provide secure access to applications.
- ? Reference: CompTIA Network+ (N10-009) Official Study Guide - Section: Secure Remote Access Technologies

NEW QUESTION: 160

An organization wants to ensure that incoming emails were sent from a trusted source. Which of the following DNS records is used to verify the source?

- A. TXT
- B. AAAA
- C. CNAME
- D. MX

Answer: ([SHOW ANSWER](#))

A TXT record can be used to store SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) information, which help verify that an email has been sent from a trusted source.

NEW QUESTION: 161

Which of the following is a type of NAC that uses a set of policies to allow or deny access to the network based on the user's identity?

- A. Standard ACL
- B. MAC filtering
- C. 802.1X
- D. SSO

Answer: ([SHOW ANSWER](#))

The correct answer is 802.1X, which is an identity-based Network Access Control (NAC) framework emphasized in the CompTIA Network+ N10-009 objectives under network security and access control. 802.1 X uses a policy-driven authentication process to determine whether a user or device is allowed network access based on verified credentials, such as usernames, passwords, or digital certificates.

802.1X operates using three main components: the supplicant (the client requesting access), the authenticator (the network device such as a switch or wireless access point), and the authentication server (typically a RADIUS server). Once the user's identity is authenticated, predefined policies determine the level of access granted-full access, limited access, or denial. This makes 802.1X a cornerstone of zero trust and enterprise-grade NAC implementations.

A standard ACL controls traffic based on IP addresses and ports, not user identity. MAC filtering allows or denies access based on device MAC addresses, which can be easily spoofed and does not verify user identity.

SSO (Single Sign-On) simplifies authentication across multiple systems but does not control network-layer access.

Network+ highlights 802.1X as a secure, scalable solution for enforcing identity-based network access policies in both wired and wireless environments.

NEW QUESTION: 162

A network consultant needs to decide between running an ethernet uplink or using the built-in 5GHz-to-point functionality on a WAP. Which of the following documents provides the best information to assist the consultant with this decision?

- A. Service-level agreement
- B. Physical diagram
- C. Logical diagram
- D. Site survey results

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 163

Which of the following is most closely associated with a dedicated link to a cloud environment and may not include encryption?

- A. Direct Connect
- B. Internet gateway
- C. Captive portal
- D. VPN

Answer: ([SHOW ANSWER](#))

Direct Connect refers to a dedicated network connection between an on-premises network and a cloud service provider (such as AWS Direct Connect). This link bypasses the public internet, providing a more reliable and higher-bandwidth connection. It may not inherently include encryption because it relies on the security measures of the dedicated physical connection itself. In contrast, other options like VPN typically involve encryption as they traverse the public internet.

Reference:

CompTIA Network+ full course material indicates that Direct Connect type services offer dedicated, private connections which might not include encryption due to the dedicated and secure nature of the link itself.

NEW QUESTION: 164

A company is opening a new site that needs to be divided into subnets that accommodate 75 hosts each.

Which of the following is the most efficient subnet?

- A. 192.168.13.0/25
- B. 192.168.13.0/26
- C. 192.168.13.0/27
- D. 192.168.13.0/28

Answer: ([SHOW ANSWER](#))

To support 75 hosts per subnet, you must choose a subnet size that provides at least 75 usable IP addresses. In IPv4, usable hosts per subnet equals $2^{(\text{host bits})} \# 2$ (subtracting network and broadcast). A /25 leaves 7 host bits ($32 - 25 = 7$), giving $2^7 \# 2 = 128 \# 2 = 126$ usable hosts, which meets the requirement and is the smallest (most efficient) option listed that does so. A /26 leaves 6 host bits, giving 62 usable hosts, which is insufficient. A /27 gives 30 usable, and a /28 gives 14 usable, both far below 75. Network+ subnetting objectives emphasize selecting the smallest subnet that satisfies the host requirement to conserve address space while meeting growth and design constraints. Therefore, 192.168.13.0/25 is the most efficient option that accommodates at least 75 hosts per subnet.

NEW QUESTION: 165

A detective is investigating an identity theft case in which the target had an RFID-protected payment card issued and compromised in the same day. The only place the target claims to have used the card was at a local convenience store. The detective notices a video camera at the store is placed in such a way that customers' credentials can be seen when they pay. Which of the following best explains this social engineering technique?

- A. Shoulder surfing
- B. Impersonation
- C. Vishing
- D. Tailgating

Answer: ([SHOW ANSWER](#))

Shoulder surfing is a social engineering attack where attackers observe someone's private information by looking over their shoulder or using tools like cameras to capture input.

From Andrew Ramdayal's guide:

"Shoulder surfing is the act of watching someone enter confidential information, such as PINs or passwords, often using direct line-of-sight or surveillance equipment."

NEW QUESTION: 166

A network technician is requesting a fiber patch cord with a connector that is round and twists to install.

Which of the following is the proper name of this connector type?

- A. ST
- B. BNC
- C. SC
- D. LC

Answer: ([**SHOW ANSWER**](#)**)**

The ST (Straight Tip) fiber connector is round with a bayonet twist-lock mechanism. It is older but still used in some fiber installations.

B). BNC is a coaxial connector.

C). SC (Subscriber Connector) is a square push-pull fiber connector.

D). LC (Lucent Connector) is a small form-factor fiber connector.

References (CompTIA Network+ N10-009):

Domain: Networking Concepts - Fiber connectors (ST, SC, LC).

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here: <https://www.edudump.com/exams/CompTIA/N10-009/premium/> (**608** Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 167

Which of the following uses the longest prefix match to determine an exit interface?

A. ARP table

B. MAC address table

C. Routing table

D. Netstat table

Answer: ([**SHOW ANSWER**](#)**)**

The longest prefix match is a routing concept used to find the most specific route to a destination IP address.

The routing table performs this calculation to determine the exit interface for a packet, ensuring the most accurate delivery. The document explains:

"Routers use the longest prefix match when searching the routing table to determine the best path for an IP packet. This ensures that the most specific (and thus optimal) route is chosen, based on the destination IP address."

NEW QUESTION: 168

Users on the network are experiencing slow throughput. A technician wants to increase throughput without changing any switch hardware. Which of the following solutions should the technician implement?

A. SVI configuration

B. VLAN trunking

C. 802.1Q tagging

D. Link aggregation

Answer: ([**SHOW ANSWER**](#)**)**

The correct answer is D. Link aggregation. Link aggregation combines multiple physical switch links into one logical connection. This increases available bandwidth and can also add redundancy, all without replacing the switch hardware itself. If users are experiencing slow throughput and the goal is to improve capacity using existing equipment, bundling links is a common and effective solution.

The other options do not directly increase throughput. SVI configuration provides Layer 3 interfaces for VLANs, but it does not add link capacity. VLAN trunking allows multiple VLANs to traverse one connection, but that does not increase bandwidth by itself. 802.1Q tagging identifies VLAN membership on tagged frames; it is related to trunking, not throughput expansion.

In many enterprise environments, link aggregation is implemented through standards such as LACP. This lets several ports act together as one logical channel, which can help distribute traffic more efficiently across the bundled interfaces. For Network+ exam scenarios, when the requirement is to improve throughput using the current switch hardware rather than buying faster switches, link aggregation is the most appropriate answer.

NEW QUESTION: 169

Which of the following network ports is used when a client accesses an SFTP server?

- A. 22**
- B. 80**
- C. 443**
- D. 3389**

Answer: A (LEAVE A REPLY)

SFTP (Secure File Transfer Protocol) operates over port 22, using SSH (Secure Shell) encryption for secure file transfers.

Breakdown of Options:

- A). 22 - Correct answer. SFTP runs over SSH (port 22) for secure file transfers.
- B). 80 - Used for HTTP, not SFTP.
- C). 443 - Used for HTTPS (secure web traffic).
- D). 3389 - Used for RDP (Remote Desktop Protocol).

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 3.1: Compare and contrast network protocols.

RFC 4253: SSH Transport Layer Protocol

NEW QUESTION: 170

Which of the following most directly secures sensitive information on a network?

- A. Data-in-transit encryption**
- B. Principle of least privilege**
- C. Role-based access controls**
- D. Multifactor authentication**

Answer: (SHOW ANSWER)

The option that most directly secures sensitive information on the network is data-in-transit encryption. This ensures that data packets are unreadable to attackers who intercept them while moving across the network.

Protocols such as TLS, HTTPS, IPsec, and SSH protect confidentiality and integrity of sensitive information.

- B). Principle of least privilege (PoLP) secures access control but does not directly protect data in motion.
- C). Role-based access control (RBAC) enforces permissions but again does not secure the data while transmitted.
- D). Multifactor authentication (MFA) strengthens identity verification but does not directly protect the data itself once transmitted.

Thus, while all options contribute to overall security, encryption of data-in-transit most directly addresses protection of sensitive information on the network.

References (CompTIA Network+ N10-009):

Domain: Network Security - Encryption methods, confidentiality, data-in-transit protection.

NEW QUESTION: 171

Which of the following is the most cost-effective way to safely expand outlet capacity in an IDF?

- A. PDU
- B. Surge protector
- C. UPS
- D. Power strip

Answer: (SHOW ANSWER)

A Power Distribution Unit (PDU) provides multiple power outlets in a data center or IDF (Intermediate Distribution Frame), while offering features like surge protection, load balancing, and sometimes remote monitoring, making it a cost-effective and reliable solution. The document confirms: "PDUs (Power Distribution Units) are a cost-effective way to expand outlet capacity in a structured cabling environment like an IDF. They ensure safe power delivery to networking equipment and often include monitoring features."

NEW QUESTION: 172

A network administrator wants users to be able to authenticate to the corporate network using a port-based authentication framework when accessing both wired and wireless devices. Which of the following is the best security feature to accomplish this task?

- A. 802.1X
- B. Access control list
- C. Port security
- D. MAC filtering

Answer: (SHOW ANSWER)

802.1X is a port-based network access control (PNAC) protocol that provides an authentication mechanism to devices wishing to connect to a LAN or WLAN. It is widely used for secure network access, ensuring that only authenticated devices can access the network, whether they are connecting via wired or wireless means.

802.1X works in conjunction with an authentication server, such as RADIUS, to validate the credentials of devices trying to connect. References: CompTIA Network+ study materials.

NEW QUESTION: 173

A network engineer needs to add a boundary network to isolate and separate the internal network from the public-facing internet. Which of the following security defense solutions would best accomplish this task?

- A. Trusted zones
- B. URL filtering
- C. ACLs
- D. Screened subnet

Answer: (SHOW ANSWER)

A screened subnet, also known as a DMZ (Demilitarized Zone), is a boundary network that separates an organization's internal network from external-facing systems. It is used to host public services like web or email servers while protecting internal systems from exposure.

Reference: Section 4.3 - Network Security Features, Defense Techniques, and Solutions - "Screened Subnet (DMZ)"

NEW QUESTION: 174

Which of the following disaster recovery concepts is calculated by dividing the total hours of operation by the total number of units?

A. MTTR

B. MTBF

C. RPO

D. RTO

Answer: B ([LEAVE A REPLY](#))

Introduction to Disaster Recovery Concepts:

Disaster recovery involves strategies and measures to ensure business continuity and data recovery in the event of a disaster.

Mean Time Between Failures (MTBF):

MTBF is a reliability metric used to predict the time between failures of a system during operation. It is calculated by dividing the total operational time by the number of failures.

Formula: $\text{MTBF} = \frac{\text{Total Operational Time}}{\text{Number of Failures}}$
MTBF=Number of FailuresTotal Operational Time This metric helps in understanding the reliability and expected lifespan of systems and components.

Example Calculation:

If a server operates for 1000 hours and experiences 2 failures, the MTBF is:

$\text{MTBF} = \frac{1000 \text{ hours}}{2} = 500 \text{ hours}$ MTBF=21000 hours=500 hours Explanation of the

Options:

A). MTTR (Mean Time to Repair): The average time required to repair a system after a failure.

B). MTBF (Mean Time Between Failures): The correct answer, representing the average time between failures.

C). RPO (Recovery Point Objective): The maximum acceptable amount of data loss measured in time.

D). RTO (Recovery Time Objective): The target time set for the recovery of IT and business activities after a disaster.

Conclusion:

MTBF is a crucial metric in disaster recovery and system reliability, helping organizations plan maintenance and predict system performance.

References:

CompTIA Network+ guide explaining MTBF, MTTR, RPO, and RTO concepts and their calculations (see page Ref 10 How to Use Cisco Packet Tracer).

NEW QUESTION: 175

A storage network requires reduced overhead and increased efficiency for the amount of data being sent.

Which of the following should an engineer likely configure to meet these requirements>?

A. Link speed

B. Jumbo frames

C. QoS

D. 802.1q tagging

Answer: ([SHOW ANSWER](#))

Jumbo frames are Ethernet frames with a payload greater than the standard maximum transmission unit (MTU) of 1500 bytes. Configuring jumbo frames can reduce overhead and increase efficiency in storage networks by allowing more data to be sent in each frame, thus reducing the number of frames needed to transmit the same amount of data.

* Reduced Overhead: By sending larger frames, the relative overhead for headers and acknowledgments is reduced.

* Increased Efficiency: Larger frames mean fewer packets to process, leading to better utilization of network bandwidth and improved performance in high-throughput environments like storage networks.

* Configuration: Requires support from all devices in the network path, including switches and network interface cards (NICs).

Network References:

* CompTIA Network+ N10-007 Official Certification Guide: Explains jumbo frames and their benefits in reducing network overhead.

* Cisco Networking Academy: Provides training on network optimization techniques, including the use of jumbo frames.

* Network+ Certification All-in-One Exam Guide: Covers advanced Ethernet features, including jumbo frames and their configuration for improved network performance.

NEW QUESTION: 176

Users at a satellite office are experiencing issues when using videoconferencing. Which of the following should a technician focus on first to rectify these issues?

A. Quality of service

B. Network signal

C. Time to live

D. Load balancing

Answer: (SHOW ANSWER)

Quality of Service (QoS) is crucial for real-time services like video conferencing. It prioritizes voice and video packets over less critical traffic (like file downloads), reducing latency, jitter, and packet loss.

B). Network signal may apply to wireless, but it's not specific to video issues.

C). Time to live (TTL) affects packet lifespan, not performance or quality.

D). Load balancing manages traffic across multiple paths but doesn't prioritize real-time traffic like QoS does.

Reference:

CompTIA Network+ N10-009 Official Objectives: 3.6 - Explain the characteristics of network topologies and types.

NEW QUESTION: 177

Which of the following network topologies contains a direct connection between every node in the network?

A. Mesh

B. Hub-and-spoke

C. Star

D. Point-to-point

Answer: A (LEAVE A REPLY)

In a mesh topology, every node is directly connected to every other node. This provides high redundancy and reliability, as there are multiple paths for data to travel between nodes. This topology is often used in networks where high availability is crucial. References: CompTIA Network+ study materials.

NEW QUESTION: 178

Which of the following should a network administrator configure when adding OT devices to an organization's architecture?

A. Honeynet

B. Data-at-rest encryption

C. Time-based authentication

D. Network segmentation

Answer: ([SHOW ANSWER](#))

Network segmentation involves dividing a network into smaller segments or subnets. This is particularly important when integrating OT (Operational Technology) devices to ensure that these devices are isolated from other parts of the network. Segmentation helps protect the OT devices from potential threats and minimizes the impact of any security incidents. It also helps manage traffic and improves overall network performance. References: CompTIA Network+ study materials.

NEW QUESTION: 179

Following a VoIP deployment, users report issues using the VoIP system. After further review, a network technician reports the following:

- * Dropped calls are occurring.
- * Local file transfer is successful.
- * New firewalls have recently been added.
- * Web traffic is functional.
- * Users experience audio latency.

Which of the following is the most likely cause of the issues?

- A. Conflicting firewall rule**
- B. Spanning tree issue**
- C. Incorrect voice VLAN**
- D. Misconfigured QoS**

Answer: ([SHOW ANSWER](#))

Misconfigured QoS is the most likely cause because the symptoms are specific to VoIP quality: dropped calls and audio latency. Voice traffic is highly sensitive to delay, jitter, and packet loss. Quality of Service allows administrators to classify and prioritize voice packets so they are handled ahead of less time-sensitive traffic such as file transfers or general web browsing. If QoS is missing or incorrectly configured, voice packets may compete equally with other traffic and suffer from congestion-related delay or loss.

The CompTIA Network+ N10-009 objectives include VoIP, QoS, traffic shaping, latency, jitter, and performance troubleshooting. The fact that local file transfers and web traffic are functional indicates the general network is working. The problem is with real-time traffic quality rather than total connectivity.

A conflicting firewall rule could block call setup or media streams, but the question emphasizes audio latency, which strongly points to QoS. A spanning tree issue would more likely cause broader Layer 2 instability. An incorrect voice VLAN could prevent phones from receiving proper addressing or access, but users are able to use the VoIP system with poor quality. Therefore, misconfigured QoS is correct.

NEW QUESTION: 180

An administrator must increase the security posture of an organization. The goal is to restrict the external-facing web server from communicating with the internal organization. Which of the following is the most cost-effective deployment?

- A. An IPS between the internet and the web server**
- B. An ACL to only allow traffic from the web server**
- C. A screened subnet for the web server**
- D. A WAF directly on the web server**

Answer: ([SHOW ANSWER](#))

A screened subnet, also commonly called a DMZ, is the best and most cost-effective deployment for isolating an external-facing web server from the internal organization. A screened subnet places publicly accessible systems in a separate network segment between the internet and the trusted internal network. Firewall rules can then strictly control what traffic is allowed between the internet, the screened subnet, and the internal network. This reduces the risk that a compromised public web server can directly communicate with or attack internal systems.

The CompTIA Network+ N10-009 objectives include network segmentation, security zones, screened subnets, firewalls, and access control. A screened subnet is a standard design for services that must be reachable from untrusted networks while protecting internal resources.

An IPS can detect or block malicious traffic, but it does not provide the same segmentation design by itself. A WAF protects web applications from application-layer attacks, but it does not necessarily prevent the web server from communicating with internal systems. An ACL may help, but a screened subnet provides the better architectural control. Therefore, the correct answer is a screened subnet for the web server.

NEW QUESTION: 181

Which of the following is used to stage copies of a website closer to geographically dispersed users?

- A. VPN
- B. CDN
- C. SAN
- D. SDN

Answer: ([SHOW ANSWER](#))

A Content Delivery Network (CDN) caches website content across multiple geographically distributed servers to reduce latency and improve load times for users worldwide.

Breakdown of Options:

- A). VPN - Encrypts network connections, does not distribute website content.
- B). CDN - # Correct answer. A network of caching servers that delivers web content faster.
- C). SAN - Storage Area Network, not related to web content distribution.
- D). SDN - Software-defined networking, which controls network flows but does not stage website content.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 1.5: Compare and contrast different networking services.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here: <https://www.edudump.com/exams/CompTIA/N10-009/premium/> (**608** Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 182

A network administrator for a small office is adding a passive IDS to its network switch for the purpose of inspecting network traffic. Which of the following should the administrator use?

- A. SNMP trap
- B. Port mirroring
- C. Syslog collection
- D. API integration

Answer: (SHOW ANSWER)

Port mirroring, also known as SPAN (Switched Port Analyzer), is used to send a copy of network packets seen on one switch port (or an entire VLAN) to another port where the IDS is connected. This allows the IDS to passively inspect network traffic without interfering with the actual traffic flow. Port mirroring is an essential feature for implementing IDS in a network for traffic analysis and security monitoring. References: CompTIA Network+ study materials.

NEW QUESTION: 183

Which of the following attacks would most likely cause duplicate IP addresses in a network?

- A.** Rogue DHCP server
- B.** DNS poisoning
- C.** Social engineering
- D.** Denial-of-service

Answer: (SHOW ANSWER)

* Definition of a Rogue DHCP Server:

* A rogue DHCP server is an unauthorized DHCP server on a network, which can assign IP addresses to devices without proper control, leading to IP address conflicts.

* Impact of a Rogue DHCP Server:

* IP Address Conflicts: Multiple devices may receive the same IP address from different DHCP servers, causing network connectivity issues.

* Network Disruption: Devices may be assigned incorrect network configuration settings, disrupting network services and connectivity.

* Comparison with Other Attacks:

* DNS poisoning: Alters DNS records to redirect traffic to malicious sites, but does not cause IP address conflicts.

* Social engineering: Involves manipulating individuals to gain unauthorized access or information, not directly related to IP address conflicts.

* Denial-of-service (DoS): Floods a network or service with excessive traffic to disrupt operations, but does not cause duplicate IP addresses.

* Prevention and Detection:

* Implement network access control measures to prevent unauthorized devices from acting as DHCP servers.

* Use DHCP snooping on switches to allow DHCP responses only from authorized DHCP servers.

References:

* CompTIA Network+ study materials on network security threats and mitigation techniques.

NEW QUESTION: 184

A network engineer configures an application server so that it automatically adjusts resource allocation as demand changes. This server will host a new application and demand is not predictable. Which of the following concepts does this scenario demonstrate?

- A.** Scalability
- B.** Software as a Service
- C.** Hybrid cloud
- D.** Elasticity

Answer: D (LEAVE A REPLY)

Elasticity is the ability of a system (often in cloud environments) to automatically scale resources up or down in real time based on demand.

A). Scalability means the ability to grow over time but not necessarily dynamically.

B). SaaS is a service model, not a resource-allocation concept.

C). Hybrid cloud is a deployment model, not a performance behavior.

References (CompTIA Network+ N10-009):

Domain: Networking Concepts - Cloud computing, elasticity vs. scalability.

NEW QUESTION: 185

Which of the following network cables involves bouncing light off of protective cladding?

- A.** Twinaxial
- B.** Coaxial
- C.** Single-mode
- D.** Multimode

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (aligned to N10-009):

Multimode fiber uses multiple paths (modes) of light that bounce off the cladding to travel through the fiber.

This is effective for shorter distances but more prone to dispersion.

- A). Twinaxial is copper, not fiber.
- B). Coaxial carries electrical signals, not light.
- C). Single-mode fiber uses a single light path directly through the core without bouncing.

References (CompTIA Network+ N10-009):

Domain: Networking Concepts - Fiber optics: single-mode vs. multimode.

NEW QUESTION: 186

A group of users cannot connect to network resources. The technician runs ipconfig from one user's device and is able to ping the gateway shown from the command. Which of the following is most likely preventing the users from accessing network resources?

- A.** VLAN hopping
- B.** Rogue DHCP
- C.** Distributed DoS
- D.** Evil twin

Answer: ([SHOW ANSWER](#))

A rogue DHCP server occurs when an unauthorized or misconfigured DHCP server assigns incorrect IP addresses, default gateways, or DNS settings to clients.

*In this scenario:

*The user can ping the gateway, meaning local network communication is working.

*However, they cannot access network resources, which suggests incorrect IP configuration (likely due to a rogue DHCP server assigning the wrong gateway or DNS).

*Why not the other options?

*VLAN hopping (A): This is an attack that exploits VLAN configurations to gain access to unauthorized VLANs. It would not typically cause multiple users to lose network access.

*Distributed DoS (C): A DDoS attack floods a network or service with traffic, but this issue is more likely misconfigured IP settings than an actual attack.

*Evil twin (D): This refers to a fraudulent Wi-Fi network mimicking a legitimate one. Since the users are on a wired network (ipconfig output checked), this is not applicable.

Reference:

NEW QUESTION: 187

A customer recently moved into a new office and notices that some wall plates are not working and are not properly labeled Which of the following tools would be best to identify the proper wiring in the IDF?

- A. Toner and probe
- B. Cable tester
- C. Visual fault locator
- D. Network tap

Answer: (SHOW ANSWER)

A toner and probe tool, also known as a tone generator and probe, is used to trace and identify individual cables within a bundle or to locate the termination points of cables in wiring closets and patch panels. It generates a tone that can be picked up by the probe, helping technicians quickly and accurately identify and label wall plates and wiring. This is the best tool for identifying proper wiring in the Intermediate Distribution Frame (IDF). References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 188

Users are reporting latency on the network. The network engineer notes the following:

Confirms the only change was a new network switch

Confirms all users are experiencing latency

Thinks the issue is a network loop caused by the lower bridge ID of the new switch Which of the following describes the next step in the troubleshooting methodology?

- A. Identify the problem.
- B. Test the theory.
- C. Implement the solution.
- D. Verify full system functionality.

Answer: (SHOW ANSWER)

The correct answer is Test the theory, which aligns directly with the CompTIA Network+ N10-009 troubleshooting methodology. According to the official troubleshooting steps, once a problem has been identified and relevant information gathered, the next step is to establish a theory of probable cause and then test that theory to determine whether it is valid.

In this scenario, the engineer has already completed the problem identification phase by confirming that all users are experiencing latency and correlating the issue with the installation of a new switch. The engineer has also formed a theory: that a network loop caused by the lower bridge ID of the new switch may be impacting Spanning Tree Protocol (STP), resulting in congestion and latency. Because this theory has already been developed, the next logical and required step is to test the theory-for example, by reviewing STP states, temporarily disabling ports, or adjusting bridge priorities.

Implementing a solution would be premature without validating the theory, and verifying full system functionality occurs only after a fix has been applied. The Network+ objectives stress following a structured methodology to avoid unnecessary changes and minimize network disruption.

Testing the theory ensures accuracy before corrective action is taken, reducing risk and downtime.

NEW QUESTION: 189

A network administrator needs to implement a solution to filter access to the internet. Which of the following should the administrator most likely implement?

- A. Router
- B. Cloud gateway
- C. Proxy
- D. Intrusion detection system

Answer: ([SHOW ANSWER](#))

A proxy server can filter internet access by controlling which websites or services users can reach. It enforces content policies and can provide caching and monitoring.

- A). A router directs traffic but doesn't filter internet sites by itself.
- B). A cloud gateway could also filter, but the most direct answer is proxy.
- D). An IDS detects suspicious activity but doesn't filter browsing access.

References (CompTIA Network+ N10-009):

Domain: Network Security - Proxy servers, filtering, access control.

NEW QUESTION: 190

A network administrator needs to implement trunk port redundancy. The change should not introduce any loops and should increase throughput. Which of the following technologies should the administrator use?

- A. Media Independent Interface with Crossover
- B. First Hop Redundancy Protocol
- C. Link Aggregation Control Protocol
- D. Spanning Tree Protocol

Answer: ([SHOW ANSWER](#))

Link Aggregation Control Protocol, or LACP, is the correct technology because it allows multiple physical links between switches to operate as one logical link. This provides redundancy and can increase throughput by distributing traffic across bundled links. If one physical link in the bundle fails, traffic can continue over the remaining links. Since the bundled links are treated as a single logical connection, LACP also helps avoid Layer 2 switching loops that would otherwise occur if multiple independent trunk links were connected between the same switches. The CompTIA Network+ N10-009 objectives include switching, trunking, redundancy, link aggregation, and loop prevention. LACP is based on IEEE 802.3ad/802.1AX and is commonly used between switches, servers, and network appliances to improve availability and bandwidth. MDIX automatically adjusts transmit and receive pairs on copper Ethernet links, but it does not provide trunk redundancy or increased throughput. First Hop Redundancy Protocol provides default gateway redundancy, not trunk link aggregation. Spanning Tree Protocol prevents loops, but it may block redundant links and does not increase throughput. Therefore, LACP is the best answer.

NEW QUESTION: 191

A network technician receives a new ticket while working on another issue. The new ticket is critical to business operations. Which of the following documents should the technician reference to determine which ticket to complete first?

- A. NDA
- B. AUP
- C. SLA
- D. MOU

Answer: C ([LEAVE A REPLY](#))

An SLA (Service Level Agreement) defines performance expectations, including response time, prioritization, and resolution time for services and support issues. It helps the technician determine which task has higher priority based on business impact.

* A. NDA (Non-Disclosure Agreement) relates to confidentiality, not task prioritization.

* B. AUP (Acceptable Use Policy) defines user behavior, not issue handling.

* D. MOU (Memorandum of Understanding) outlines informal agreements and doesn't define ticket priorities.

#Reference:

CompTIA Network+ N10-009 Official Objectives: 4.1 - Compare and contrast common documentation types.

NEW QUESTION: 192

Which of the following is the best use case of a site-to-site VPN?

A. Securing access across an untrusted network

B. Encrypting data at rest

C. Filtering traffic between two internal subnets

D. Hosting public-facing applications that contain company resources

Answer: ([SHOW ANSWER](#))

A site-to-site VPN is used to securely connect two networks over an untrusted network, most commonly the public internet. In Network+ (N10-009) objectives, VPNs are described as providing confidentiality and integrity for data in transit by creating an encrypted tunnel between sites (for example, headquarters and a branch office). This allows systems at both locations to communicate as if on the same private WAN, while preventing eavesdropping or tampering by intermediate networks. Typical implementations use IPsec tunneling and rely on negotiated encryption/authentication parameters to protect traffic end-to-end between VPN gateways.

Encrypting data at rest refers to storage encryption (disk/database), not VPN tunneling. Filtering traffic between two internal subnets is usually handled by ACLs, firewalls, or segmentation controls, not a site-to-site VPN. Hosting public-facing applications is a DMZ / reverse proxy / WAF design concern; a VPN is not the primary control for exposing public services (and generally you would not require the public to use a VPN to reach a public website). Therefore, securing site connectivity across an untrusted network is the best match.

NEW QUESTION: 193

A network technician needs to resolve some issues with a customer's SOHO network. The customer reports that some of the PCs are not connecting to the network, while others appear to be working as intended.

INSTRUCTIONS

Troubleshoot all the network components.

Review the cable test results first, then diagnose by clicking on the appropriate PC, server, and Layer 2 switch.

Identify any components with a problem and recommend a solution to correct each problem.

If at any time you would like to bring back

the initial state of the simulation, please

click the Reset All button.

Cable Test Results



Switch 1

Length : 16M

Port : GigabitEthernet0/5

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

Connected to Switch 2

PC1

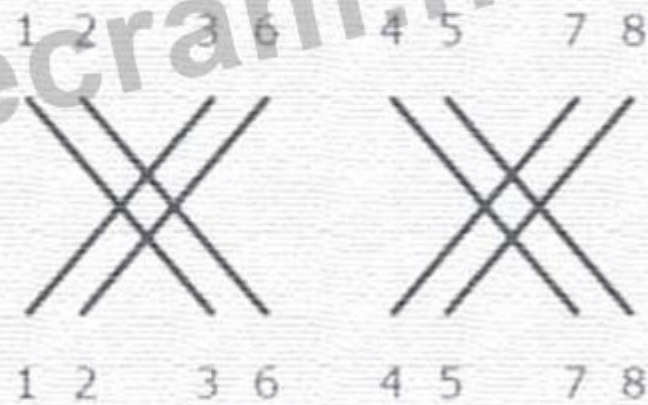
PC2

PC3

PC4

PC5

PC6



CompTIA

Cable Test Results



Switch 1

Length : 16M

Port : GigabitEthernet0/5

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

Connected to Switch 1

PC1

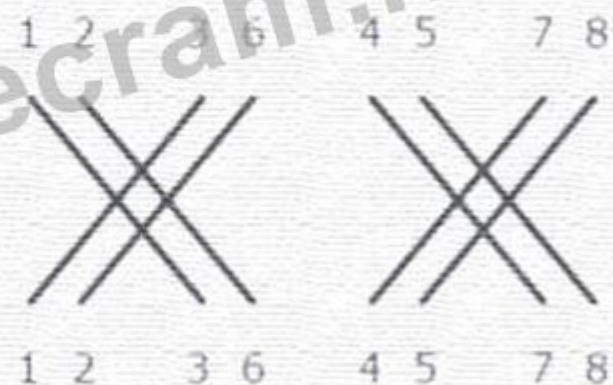
PC2

PC3

PC4

PC5

PC6



Cable Test Results



Switch 1

Length : 22M

Port : GigabitEthernet0/1

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

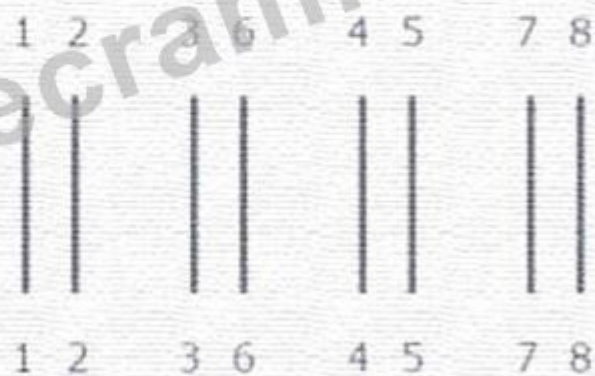
PC2

PC3

PC4

PC5

PC6



CompTIA

Cable Test Results

Switch 1

Switch 2

Server

PC1

PC2

PC3

PC4

PC5

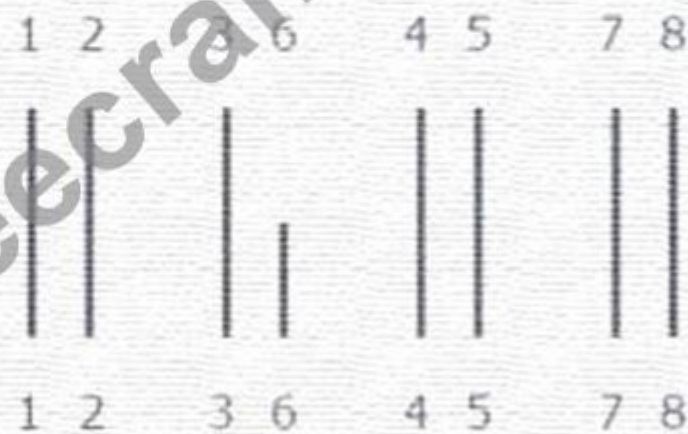
PC6

Length : 12M

Port : GigabitEthernet0/1

VLAN : VLAN 10

Speed : 1000 FDX



Cable Test Results

Switch 1

Switch 2

Server

PC1

PC2

PC3

PC4

PC5

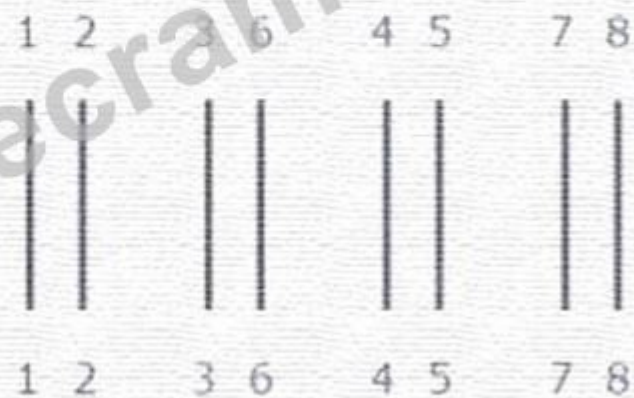
PC6

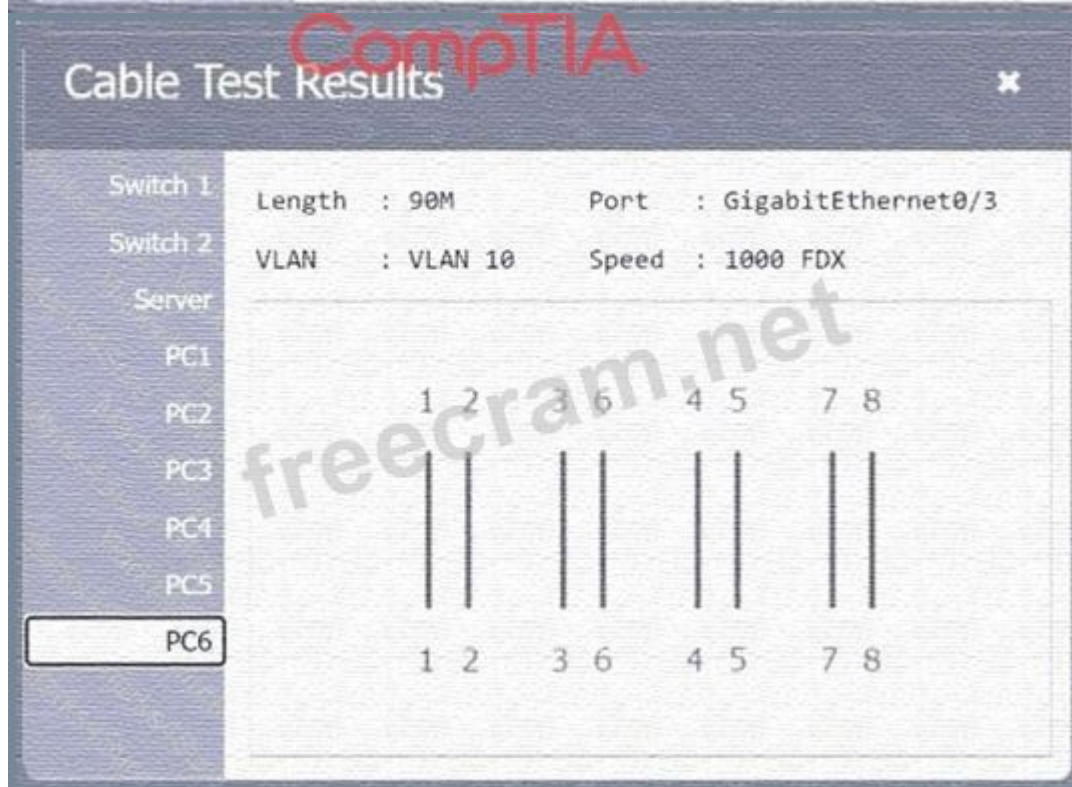
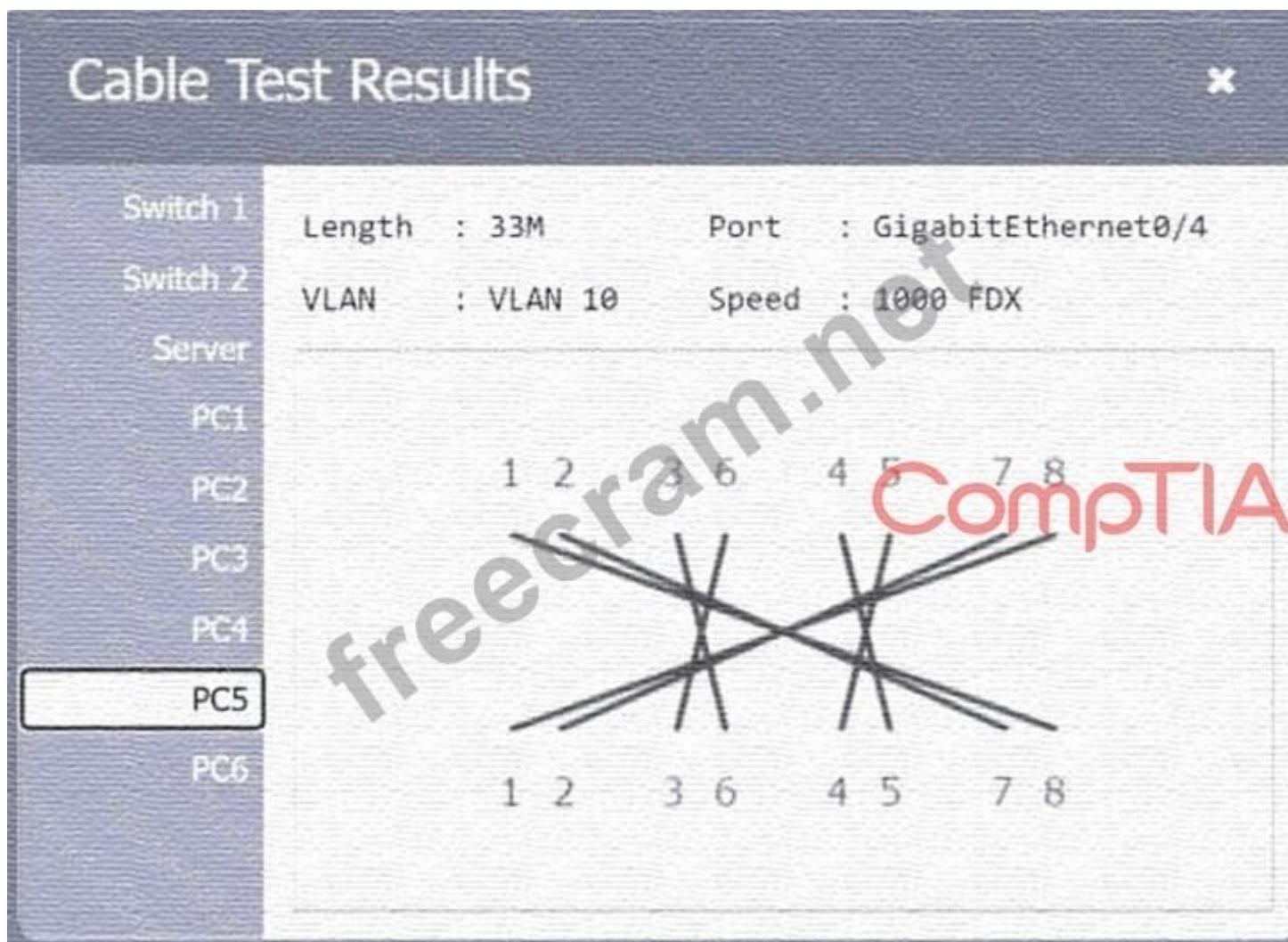
Length : 18M

Port : GigabitEthernet0/3

VLAN : VLAN 11

Speed : 1000 FDX



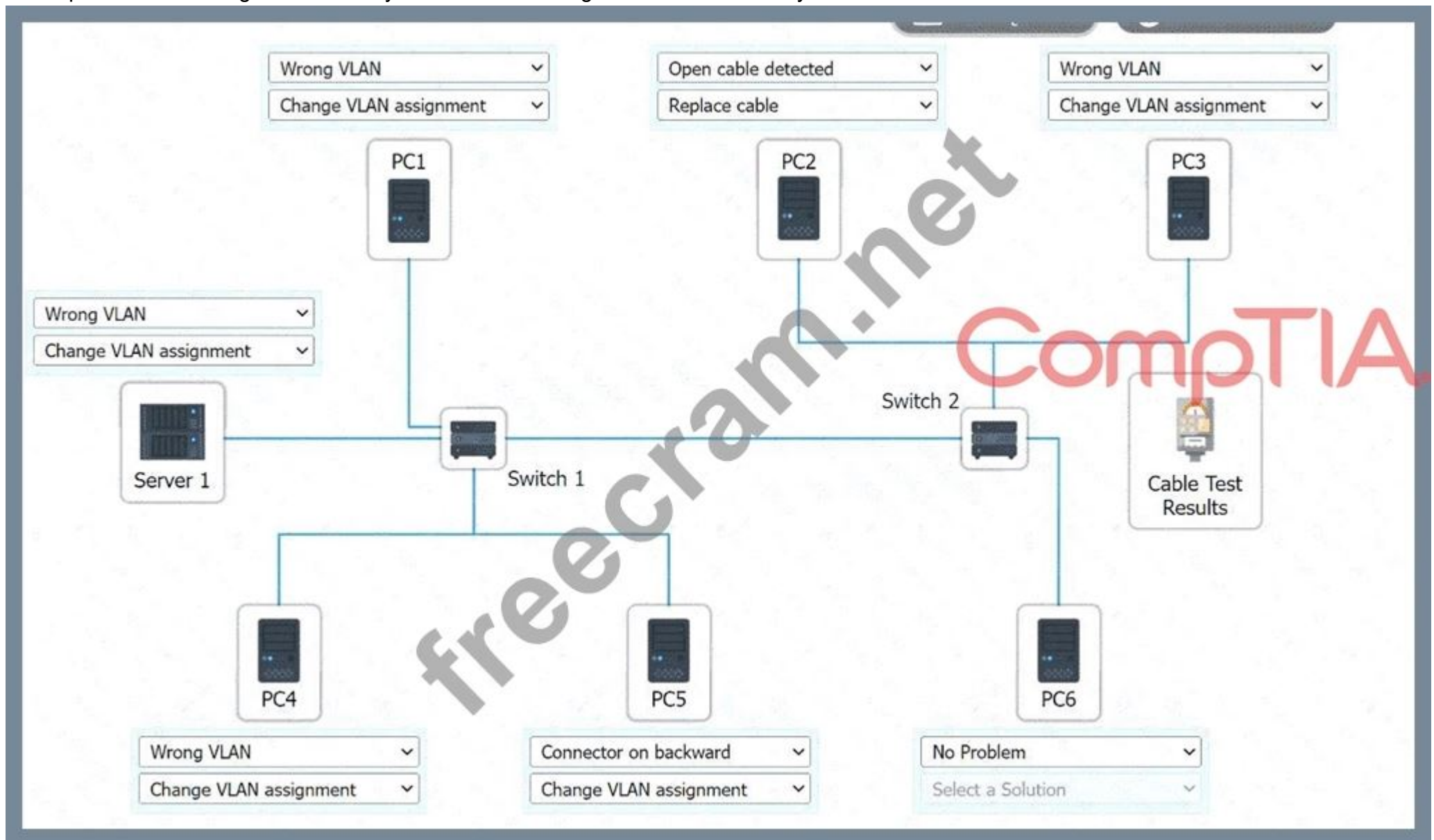


Answer:

See the answer and solution below:

Explanation:

A computer network diagram with many boxes and text AI-generated content may be incorrect.



NEW QUESTION: 194

Which of the following should a company implement in order to share a single IP address among all the employees in the office?

- A. STP
- B. BGP
- C. PAT
- D. VXLAN

Answer: ([SHOW ANSWER](#))

PAT (Port Address Translation) allows multiple devices on a local network to share a single public IP address when accessing the internet. It translates the private IP addresses to a single public IP with different port numbers for each session. The document states:

"PAT (Port Address Translation) allows multiple devices on a LAN to share a single public IP address by assigning unique port numbers to each session, enabling internet connectivity for all devices."

NEW QUESTION: 195

A network engineer needs to correlate findings and receive alerts if there are brute force attacks, DDoS attacks, or port scanning happening within their network. Which of the following network monitoring technologies should the engineer implement?

- A. Packet capture
- B. SNMPv3
- C. SIEM
- D. Syslog collector

Answer: (SHOW ANSWER)

A SIEM (Security Information and Event Management) platform is built to collect, correlate, and alert on security-relevant events across many sources, which is exactly what's needed to identify patterns such as brute force attempts, port scanning, and DDoS indicators. In Network+ (N10-009) security operations concepts, correlation is key: a SIEM can ingest logs from firewalls, IDS/IPS, servers, authentication systems, endpoint agents, and network devices, then apply rules/analytics to detect suspicious behavior that might not be obvious from a single log source. It can also generate real-time alerts, dashboards, and incident timelines-helping the engineer respond quickly and prioritize threats.

Packet capture provides deep visibility into traffic but is not inherently designed for enterprise-wide correlation and alerting without significant additional tooling and expertise. SNMPv3 is used for secure device monitoring (status, counters, performance) rather than detecting coordinated attack patterns. A syslog collector centralizes logs but generally does not provide the same level of correlation, enrichment, and automated alerting capabilities as a SIEM. Therefore, SIEM is the best answer.

NEW QUESTION: 196

Which of the following connection methods allows a network engineer to automate the configuration deployment for network devices across the environment?

- A. RDP
- B. Telnet
- C. GUI
- D. API

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation (aligned to N10-009):

APIs (Application Programming Interfaces) allow automation tools and scripts to push configurations to network devices programmatically. Modern network automation platforms rely on APIs to ensure consistency and scalability.

A). RDP is remote desktop for Windows systems, not automation.

B). Telnet is insecure and manual.

C). GUI requires manual configuration, not automation.

References (CompTIA Network+ N10-009):

Domain: Network Operations - Automation, orchestration, APIs in network management.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here: <https://www.edudump.com/exams/CompTIA/N10-009/premium/> (608 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 197

Which of the following connection methods allows a network engineer to automate configuration deployment for network devices across the environment?

- A. RDP
- B. Telnet
- C. SSH
- D. GUI

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):

SSH provides secure, scriptable remote access used by automation/orchestration tools (e.g., leveraging CLI, NETCONF over SSH, or Ansible modules) to push configurations at scale.

- * A. RDP is primarily for Windows GUI sessions and is not commonly used for network device automation.
- * B. Telnet can be scripted but is insecure (plaintext); modern best practice is to use SSH.
- * D. GUI access is typically manual and not ideal for scalable, repeatable automation.

References (CompTIA Network+ N10-009):

* Domain: Network Operations - Configuration management, automation/orchestration, secure management protocols (SSH vs. Telnet), change at scale.

NEW QUESTION: 198

A new network is being created to support 126 users. Which of the following CIDR ranges provides the most efficient use of space?

- A. 10.2.2.0/23
- B. 10.2.2.0/24
- C. 10.2.2.0/25
- D. 10.2.2.0/26

Answer: (SHOW ANSWER)

To support 126 users, the subnet must provide at least 126 usable host addresses. In IPv4 subnetting, usable hosts are calculated as: $(2^{\text{host bits}}) - 2$, subtracting the network and broadcast addresses.

A /25 leaves 7 host bits (because $32 - 25 = 7$). That yields $2^7 = 128$ total addresses, and $128 - 2 = 126$ usable—an exact fit and therefore the most efficient option listed.

A /24 provides 256 total addresses and 254 usable, which would waste more addresses than necessary. A /23 provides 512 total addresses and 510 usable—far more waste. A /26 leaves 6 host bits, giving 64 total addresses and 62 usable, which is not enough for 126 users.

The 10.2.2.0 address is within the private 10.0.0.0/8 range, so it's appropriate for internal addressing.

Therefore, 10.2.2.0/25 is the correct CIDR range for efficiently supporting 126 hosts.

NEW QUESTION: 199

During a security audit, a consulting firm notices inconsistencies between the documentation and the actual environment. Which of the following can keep a record of who made the changes and what the changes are?

- A. Network access control
- B. Configuration monitoring
- C. Zero Trust
- D. Syslog

Answer: ([SHOW ANSWER](#))

Configuration monitoring and management tools (often part of network management systems) maintain version-controlled records of device configurations, track changes, and log who made them. This provides accountability and supports compliance audits.

A). Network access control (NAC) manages endpoint access policies but does not track device config changes.

C). Zero Trust is a security framework requiring strict identity verification, not a configuration tracking tool.

D). Syslog collects system logs, but without a config monitoring system, it does not directly compare documentation to device state.

References (CompTIA Network+ N10-009):

Domain: Network Operations - Change management, configuration management, auditing.

NEW QUESTION: 200

A network engineer needs to deploy an access point at a remote office so that it will not communicate back to the wireless LAN controller. Which of the following deployment methods must the engineer use to accomplish this task?

A. Lightweight

B. Autonomous

C. Mesh

D. Ad hoc

Answer: ([SHOW ANSWER](#))

Autonomous access points operate independently without needing to communicate with a central wireless LAN controller. This is ideal for remote deployments.

From Andrew Ramdayal's guide:

"Autonomous access points are stand-alone devices that manage their own configurations and operations.

They do not require a WLC and are ideal for small or remote office deployments."

NEW QUESTION: 201

Which of the following is a use case for a PaaS environment?

A. Mobile access

B. E-commerce site

C. Application development

D. Cloud-native software

Answer: ([SHOW ANSWER](#))

PaaS (Platform as a Service) is best suited for application development because it provides a managed platform that includes the runtime environment, development frameworks, middleware, databases (often), and build/deployment tooling. In a PaaS model, the cloud provider manages the underlying infrastructure (servers, storage, networking, OS patching, and often the application runtime), allowing developers to focus on writing code, testing, and releasing applications quickly. This aligns with Network+ cloud concepts where service models are compared by responsibility: PaaS reduces operational overhead for the customer and accelerates development through standardized environments and automation.

Mobile access is a use case for remote access solutions (VPN, zero trust access, MDM), not specifically PaaS.

An e-commerce site could be hosted using many models (IaaS, PaaS, SaaS), so it's not the most specific match. Cloud-native software describes an architectural style (microservices, containers, managed services) and can be built using PaaS components, but it is broader than a single "use

case" and is not as directly tied to the PaaS definition as application development is. Therefore, application development is the clearest and most accurate PaaS use case.

NEW QUESTION: 202

A small company has the following IP addressing strategy:

A user is unable to connect to the company fileshare server located at 192.168.10.1. The user's networking configuration is:

Which of the following will most likely correct the issue?

- A.** Changing the IPv4 address to 192.168.10.1
- B.** Changing the subnet mask to 255.255.255.0
- C.** Changing the DNS servers to internet IPs
- D.** Changing the physical address to 7A-01-7A-21-01-50

Answer: ([SHOW ANSWER](#))

If the user cannot communicate with 192.168.10.1, they might be on a different subnet. Changing the subnet mask to 255.255.255.0 ensures the user and the file server are in the same subnet.

Breakdown of Options:

A: Changing the IPv4 address to 192.168.10.1 - This would conflict with the server's IP.

B: Changing the subnet mask to 255.255.255.0 - # Correct answer. Ensures both the user and the server are on the same subnet.

C: Changing the DNS servers - DNS does not affect local network connectivity.

D: Changing the physical address - The MAC address does not impact subnet communication.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 2.4: Explain subnetting and addressing concepts.

NEW QUESTION: 203

A network administrator wants to implement security zones in the corporate network to control access to only individuals inside of the corporation.

Which of the following security zones is the best solution?

- A.** Extranet
- B.** Trusted
- C.** VPN
- D.** Public

Answer: ([SHOW ANSWER](#))

Introduction to Security Zones:

Security zones are logical segments within a network designed to enforce security policies and control access.

They help in segregating and securing different parts of the network.

Types of Security Zones:

Trusted Zone: This is the most secure zone, typically used for internal corporate networks where only trusted users have access.

Extranet: This zone allows controlled access to external partners, vendors, or customers.

VPN (Virtual Private Network): While VPNs are used to create secure connections over the internet, they are not a security zone themselves.

Public Zone: This zone is the least secure and is typically used for public-facing services accessible by anyone.

Trusted Zone Implementation:

The trusted zone is configured to include internal corporate users and resources. Access controls, firewalls, and other security measures ensure that only authorized personnel can access this zone.

Internal network segments, such as the finance department, HR, and other critical functions, are usually placed in the trusted zone.

Example Configuration:

Firewall Rules: Set up rules to allow traffic only from internal IP addresses.

Access Control Lists (ACLs): Implement ACLs on routers and switches to restrict access based on IP addresses and other criteria.

Segmentation: Use VLANs and subnetting to segment and isolate the trusted zone from other zones.

Explanation of the Options:

A). Extranet: Suitable for external partners, not for internal-only access.

B). Trusted: The correct answer, as it provides controlled access to internal corporate users.

C). VPN: A method for secure remote access, not a security zone itself.

D). Public: Suitable for public access, not for internal corporate users.

Conclusion:

Implementing a trusted zone is the best solution for controlling access within a corporate network. It ensures that only trusted internal users can access sensitive resources, enhancing network security.

References:

CompTIA Network+ guide detailing security zones and their implementation in a corporate network (see page Ref 9 Basic Configuration Commands).

NEW QUESTION: 204

A network administrator is configuring a network for a new site that will have 150 users. Within the next year, the site is expected to grow by ten users. Each user will have two IP addresses, one for a computer and one for a phone connected to the network. Which of the following classful IPv4 address ranges will be best- suited for the network?

A. Class D

B. Class B

C. Class A

D. Class C

Answer: (SHOW ANSWER)

IPv4 addresses are divided into classes:

Class A: Supports 16,777,214 hosts (large enterprises).

Class B: Supports 65,534 hosts (medium to large networks).

Class C: Supports 254 hosts (small to medium networks).

Class D: Used for multicast, not for assigning IPs to hosts.

Step-by-step Calculation:

The network will have 150 users initially, with a projected growth of 10 users, totaling 160 users.

Each user has two devices, so $160 \times 2 = 320$ IP addresses needed.

A Class C subnet has 254 usable IPs by default, which is not sufficient.

A Class B subnet can support thousands of hosts, making it the most appropriate option.

Incorrect Options:

A). Class D: Reserved for multicast, not for host assignments.

C). Class A: Overkill for a network of this size.

D). Class C: Cannot support 320 hosts without subnetting, making Class B the best choice.

Reference:

NEW QUESTION: 205

A network technician is designing a LAN for a new facility. The company is expecting more than 300 devices to connect to the network. Which of the following masks will provide the most efficient subnet?

- A. 255.255.0.0
- B. 255.255.192.0
- C. 255.255.254.0
- D. 255.255.255.254

Answer: ([SHOW ANSWER](#))

The requirement is to support over 300 hosts. The subnet mask 255.255.254.0 (or /23) provides 512 addresses, 510 of which are usable - ideal for around 300 devices.

- * 255.255.0.0 (/16) provides too many addresses.
- * 255.255.192.0 (/18) gives 16384 addresses - overkill.
- * 255.255.255.254 is invalid for host assignments (only 2 addresses, 0 usable).

From Andrew Ramdayal's guide:

"To support 300 hosts, a /23 subnet (255.255.254.0) offers 510 usable addresses - the most efficient choice without excessive overhead."

NEW QUESTION: 206

A laptop user gets an error when trying to access the company 's intranet site. A technician runs ipconfig /all with the following results:

Autoconfiguration IPv4 Address: 169.254.0.5 (Preferred)

Subnet Mask: 255.255.0.0

Default Gateway:

DHCP Server:

Which of the following is most likely causing the issue?

- A. Short DHCP lease duration
- B. IIS server malfunction
- C. Address pool exhaustion
- D. IDS misconfiguration

Answer: ([SHOW ANSWER](#))

The correct answer is C. Address pool exhaustion. The client has an address in the 169.254.x.x range, which is an APIPA address automatically assigned when a system cannot get a valid IP lease from DHCP. The absence of both a default gateway and a DHCP server entry confirms that the laptop did not receive proper network settings from the DHCP service.

Among the choices, the most likely cause is that the DHCP server has no addresses left in its scope. When the address pool is exhausted, new or renewing clients cannot obtain a lease and must self-assign an APIPA address instead. A client with that kind of address cannot normally reach internal resources such as an intranet site because it lacks the correct network configuration.

The other options do not align with the evidence shown. A short DHCP lease duration could create frequent renewals, but it does not directly explain this output. An IIS malfunction would affect the web server, not the client's IP assignment. An IDS misconfiguration would not normally cause a host to self-assign a 169.254 address.

This is a DHCP-related problem, and from the available answers, address pool exhaustion is the best explanation.

NEW QUESTION: 207

A network technician is investigating an issue in which a specific user is unable to access a server. Other users in the company, however, can access the server. After checking the switch and router logs, the technician is unable to identify any issues. Which of the following troubleshooting steps should the technician take next?

- A. Inspect the client's firewall configuration
- B. Update the network equipment's firmware
- C. Check the server's DNS configuration
- D. Check the server's event logs

Answer: ([SHOW ANSWER](#))

The technician should inspect the client's firewall configuration. Since only one specific user is unable to access the server while other users can access it successfully, the issue is most likely isolated to that user's device, account, local configuration, or local security settings. After switch and router logs show no network infrastructure issue, the next logical step is to examine the affected client.

The CompTIA Network+ N10-009 troubleshooting methodology emphasizes identifying the scope of the problem, testing the most likely causes, and isolating whether the issue is client-side, server-side, or network-side. A local firewall could block outbound connections to the server, block a required application, restrict ports, or apply a profile that prevents communication.

Updating network firmware is not an appropriate next step because there is no evidence of a widespread infrastructure problem. Checking the server's DNS configuration is unlikely because other users can access the same server. Checking the server's event logs may be useful later, but the scenario points first to the single affected client. Therefore, inspecting the client's firewall configuration is the best next troubleshooting step.

NEW QUESTION: 208

After installing a new wireless access point, an engineer tests the device and sees that it is not performing at the rated speeds. Which of the following should the engineer do to troubleshoot the issue? (Select two.)

- A. Ensure a bottleneck is not coming from other devices on the network.
- B. Install the latest firmware for the device.
- C. Create a new VLAN for the access point.
- D. Make sure the SSID is not longer than 16 characters.
- E. Configure the AP in autonomous mode.
- F. Install a wireless LAN controller.

Answer: ([SHOW ANSWER](#))

Troubleshooting poor performance of a newly installed access point involves multiple steps. Checking for network bottlenecks and ensuring the device firmware is up to date are crucial first steps. The document confirms: "Network bottlenecks can severely limit the performance of even the fastest wireless access points, so it's essential to verify that no other devices are causing a slowdown. In addition, keeping firmware updated ensures optimal performance and security."

NEW QUESTION: 209

Which of the following cloud platform technology characteristics would a quantum computing host most likely prioritize?

- A. Scalability
- B. Elasticity
- C. Multitenancy
- D. Cost

Answer: ([SHOW ANSWER](#))

The best answer is B. Elasticity . Quantum computing workloads are highly specialized and often require access to extremely expensive, limited, and on-demand processing resources. In cloud terms, elasticity is the ability to rapidly allocate and release resources as demand changes. That makes it a strong fit for environments where usage may spike for short periods and then drop off again.

A quantum host would not usually be designed around ordinary shared-office priorities. Instead, it would favor the ability to obtain powerful compute capacity exactly when needed, without keeping that level of capacity permanently assigned. That is the practical value of elasticity in a cloud model.

Scalability is close, but it usually describes the broader ability to increase capacity over time or as demand grows. Elasticity is more specific to dynamic, responsive adjustment of resources, which matches specialized compute workloads much better. Multitenancy refers to multiple customers sharing underlying infrastructure, and cost is always important, but neither is the main technical characteristic being highlighted here. For exam purposes, when a scenario describes advanced or highly variable compute demand in the cloud, elasticity is usually the strongest answer because it focuses on rapid resource expansion and reduction as needed.

NEW QUESTION: 210

Which of the following layers of the OSI model is responsible for end-to-end encryption?

- A. Presentation
- B. Application
- C. Session
- D. Transport

Answer: (SHOW ANSWER)

The correct answer is Presentation, which is Layer 6 of the OSI model. According to the CompTIA Network+ N10-009 objectives, the Presentation layer is responsible for data formatting, compression, and encryption, ensuring that data sent from the application layer of one system can be properly interpreted by the receiving system.

End-to-end encryption refers to encrypting data before transmission and decrypting it only at the final destination, preventing intermediaries from accessing the plaintext data. In the OSI model, this encryption and decryption function is logically placed at the Presentation layer, which sits between the Application and Session layers. This layer transforms data into a standardized format and applies security mechanisms such as encryption algorithms.

While modern implementations like TLS/SSL often operate across multiple layers in real-world networking stacks, the Network+ exam adheres to the conceptual OSI model when testing knowledge. From an OSI perspective, encryption is explicitly associated with the Presentation layer.

The Application layer provides network services to end-user applications, the Session layer manages session establishment and teardown, and the Transport layer focuses on segmentation, flow control, and reliability.

None of these layers are primarily responsible for encryption within the OSI framework.

CompTIA emphasizes understanding these conceptual responsibilities, making Presentation the correct and expected answer.

NEW QUESTION: 211

Which of the following allows for the interception of traffic between the source and destination?

- A. Self-signed certificate
- B. VLAN hopping
- C. On-path attack
- D. Phishing

Answer: (SHOW ANSWER)

An on-path attack (formerly known as a man-in-the-middle (MITM) attack) involves intercepting and potentially altering communications between two parties without their knowledge. This can be done via techniques like ARP poisoning, rogue access points, or SSL stripping.

Breakdown of Options:

- A). Self-signed certificate - These are untrusted SSL certificates but do not intercept traffic.
- B). VLAN hopping - VLAN hopping exploits VLAN misconfigurations but does not necessarily intercept communications.
- C). On-path attack - Correct answer. This intercepts and modifies traffic between two endpoints.
- D). Phishing - Phishing tricks users into revealing credentials rather than intercepting network traffic.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 3.2: Explain common security concepts.

NIST SP 800-115: Guide to Security Testing and Assessments

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here: <https://www.edudump.com/exams/CompTIA/N10-009/premium/> (608 Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 212

Developers want to create a mobile application that requires a runtime environment, developer tools, and databases. The developers will not be responsible for security patches and updates. Which of the following models meets these requirements?

- A. Container as a service
- B. Infrastructure as a service
- C. Platform as a service
- D. Software as a service

Answer: (SHOW ANSWER)

The correct answer is Platform as a Service (PaaS). PaaS provides developers with a ready-to-use platform that includes runtime environments, developer tools, middleware, and database services. Developers can focus on writing code while the provider handles security patches, updates, and infrastructure management.

- A). CaaS (Containers as a Service) focuses on deploying and managing containerized applications, not providing full developer platforms.
- B). IaaS delivers virtual machines, storage, and networking, but administrators must install and maintain the OS, middleware, and updates.
- D). SaaS provides end-user applications (e.g., email, CRM), not platforms for development.

By using PaaS, the developers can build applications quickly and cost-effectively without worrying about underlying infrastructure or system maintenance.

References (CompTIA Network+ N10-009):

Domain: Networking Concepts - Cloud service models (IaaS, PaaS, SaaS, CaaS).

NEW QUESTION: 213

Which of the following protocols has a default administrative distance value of 90?

- A. RIP
- B. EIGRP

C. OSPF

D. BGP

Answer: B ([LEAVE A REPLY](#))

EIGRP (Enhanced Interior Gateway Routing Protocol) has a default administrative distance (AD) value of 90 for internal routes. The administrative distance is used to rate the trustworthiness of routing information received from different routing protocols. EIGRP, developed by Cisco, has an AD of 90, which is lower than that of RIP (120) and OSPF (110), making it more preferred if multiple protocols provide a route to the same destination. References: CompTIA Network+ study materials.

NEW QUESTION: 214

A Chief Executive Officer (CEO) of a company purchases a new phone that will be used while traveling to different countries. The CEO needs to be able to place outgoing calls and receive incoming calls on the phone using a SIM card. Which of the following cellular technologies does the CEO's phone need?

A. WDMA

B. CDMA

C. GSM

D. SLA

Answer: ([SHOW ANSWER](#)**)**

GSM (Global System for Mobile communications) is the international standard that uses SIM cards to authenticate and connect phones to the cellular network. GSM allows users to place and receive calls while traveling globally, provided they have a SIM card. CDMA, on the other hand, does not use SIM cards in the same way and is primarily used in the United States. (Reference: CompTIA Network+ Study Guide, Chapter on Network Fundamentals)

NEW QUESTION: 215

A network engineer is configuring network ports in a public office. To increase security, the engineer wants the ports to allow network connections only after authentication. Which of the following security features should the engineer use?

A. Port security

B. 802.1X

C. MAC filtering

D. Access control list

Answer: ([SHOW ANSWER](#)**)**

802.1X provides port-based Network Access Control (NAC). Ports remain in a blocked state until a device authenticates (usually with RADIUS). This is ideal for public or semi-public areas where ports should not be "always on."

A). Port security restricts by MAC addresses but does not authenticate users.

C). MAC filtering is easily spoofed and weaker than 802.1X.

D). ACLs filter traffic but do not enforce port-based authentication.

References (CompTIA Network+ N10-009):

Domain: Network Security - NAC, 802.1X authentication, port-based security.

NEW QUESTION: 216

Which of the following internal routing protocols is best characterized as having fast convergence and being loop-free?

- A. BGP
- B. STP
- C. OSPF
- D. RIP

Answer: ([SHOW ANSWER](#))

The correct answer is OSPF (Open Shortest Path First). OSPF is a link-state routing protocol known for its fast convergence and use of the Dijkstra algorithm to calculate the shortest loop-free path. It efficiently scales to large enterprise networks and avoids routing loops by maintaining a complete topology map.

A). BGP is primarily an external routing protocol used between ISPs, not internal.

B). STP is not a routing protocol; it prevents loops at Layer 2.

D). RIP is an older distance-vector protocol with slower convergence and a maximum hop limit of 15.

OSPF's design makes it the preferred internal gateway protocol (IGP) for medium-to-large organizations requiring speed and loop-free reliability.

References (CompTIA Network+ N10-009):

Domain: Networking Concepts - IGPs, OSPF, routing protocols.

NEW QUESTION: 217

Which of the following is a best practice when a hardware device reaches its end of life?

- A. Purchasing an extended warranty and support
- B. Decommissioning and replacing the device
- C. Selling or donating the device
- D. Using the device for testing and training

Answer: B ([LEAVE A REPLY](#))

When a hardware device reaches end of life, or EOL, the best practice is to decommission and replace it. EOL devices may no longer receive vendor support, firmware updates, security patches, replacement parts, or compatibility updates. Continuing to use unsupported infrastructure can introduce operational risk, security vulnerabilities, compliance issues, and increased downtime. In network environments, unsupported switches, routers, firewalls, wireless access points, and servers can become weak points in the organization's infrastructure.

The CompTIA Network+ N10-009 objectives include lifecycle management, documentation, risk management, and operational best practices.

Replacing EOL hardware ensures that the network remains supportable, secure, and aligned with vendor recommendations. Purchasing an extended warranty may not be possible once a device is fully EOL, and even extended support does not always include security or feature updates. Selling or donating the device may create data-handling and security concerns if it is not properly sanitized. Using the device for testing and training may be acceptable in isolated labs, but it is not the best practice for production infrastructure. Therefore, replacement and decommissioning is the correct answer.

NEW QUESTION: 218

A network technician is examining the configuration on an access port and notices more than one VLAN has been set. Which of the following best describes how the port is configured?

- A. With a voice VLAN
- B. With too many VLANs
- C. With a default VLAN
- D. With a native VLAN

Answer: ([SHOW ANSWER](#))

It is common for an access port to have both a voice VLAN and a data VLAN. A voice VLAN separates voice traffic from regular data traffic, ensuring better quality and security for voice communications.

NEW QUESTION: 219

A network engineer queries a hostname using dig, and a valid IP address is returned. However, when the engineer queries that same IP address using dig, no hostname is returned. Which of the following DNS records is missing?

- A. MX
- B. CNAME
- C. AAAA
- D. PTR

Answer: ([SHOW ANSWER](#))

This scenario describes a successful forward DNS lookup (hostname # IP address) but a failed reverse DNS lookup (IP address # hostname). Reverse lookups rely on a PTR (Pointer) record, which is stored in a reverse lookup zone (in-addr.arpa for IPv4, ip6.arpa for IPv6). If the engineer can resolve the hostname to an IP, that indicates an A record (or possibly AAAA for IPv6) exists and is functioning. But when querying the IP directly and receiving no hostname, the most likely issue is that the reverse mapping is not configured- meaning the PTR record is missing. An MX record is used for mail exchange routing, not hostname resolution. A CNAME provides an alias from one hostname to another and does not create reverse mappings. An AAAA record maps a hostname to an IPv6 address; it is not used for reverse lookups of an IP to a name. Network+ objectives emphasize understanding common DNS record types and the difference between forward and reverse resolution, making PTR the correct missing record here.

NEW QUESTION: 220

Which of the following is the most cost-effective way for a network administrator to establish a persistent, secure connection between two facilities?

- A. Site-to-site VPN
- B. GRE tunnel
- C. VXLAN
- D. Dedicated line

Answer: ([SHOW ANSWER](#))

A Site-to-site VPN (Virtual Private Network) is the most cost-effective solution for establishing a persistent, secure connection between two facilities. It uses the public internet to create an encrypted tunnel, leveraging existing internet connections without requiring expensive dedicated infrastructure. This makes it ideal for organizations looking to securely connect remote sites while minimizing costs.

Why not GRE tunnel? Generic Routing Encapsulation (GRE) tunnels encapsulate traffic but do not provide encryption natively, requiring additional protocols (e.g., IPsec) for security. This adds complexity and is less cost-effective than a site-to-site VPN, which integrates encryption.

Why not VXLAN? Virtual Extensible LAN (VXLAN) is used for overlay networks in data centers to extend Layer 2 networks, not for secure site-to-site connectivity.

Why not Dedicated line? A dedicated line (e.g., leased line or MPLS) provides high reliability but is significantly more expensive due to the need for dedicated infrastructure.

Reference: CompTIA Network+ N10-009 Objective 1.7: Explain the use cases for virtual private networks (VPNs) and tunneling protocols. The CompTIA Network+ Study Guide (e.g., Chapter 12: Network Security) explains that site-to-site VPNs are a cost-effective, secure method for connecting geographically separate networks over the internet.

NEW QUESTION: 221

Which of the following allows a remote user to connect to the network?

- A. Command-line interface
- B. API gateway
- C. Client-to-site VPN
- D. Jump box

Answer: ([SHOW ANSWER](#))

A Client-to-Site VPN allows a remote user to securely connect to a company's internal network, providing access as if they were physically on-site.

NEW QUESTION: 222

The leadership team is updated on the results of an approved change request after a breach. Which of the following troubleshooting methodology steps is described in this example?

- A. Establishing a theory of probable cause
- B. Implementing the solution or escalating as necessary
- C. Documenting findings, actions, outcomes, and lessons learned throughout the process
- D. Establishing a plan of action to resolve the problem and identifying potential effects

Answer: ([SHOW ANSWER](#))

The correct answer is C. Documenting findings, actions, outcomes, and lessons learned throughout the process. According to the CompTIA Network+ N10-009 troubleshooting methodology, the final step in the structured troubleshooting process involves documenting everything that occurred during the incident. This includes the root cause, actions taken, changes implemented (such as approved change requests), outcomes of those actions, and any lessons learned.

In the scenario, the key phrase is that leadership is being updated on the results after a breach and an approved change request. This clearly aligns with post-resolution communication and documentation, where technical teams report findings and outcomes to stakeholders. This step is critical for organizational knowledge, audit requirements, compliance, and improving future incident response.

The other options represent earlier steps in the troubleshooting process. Establishing a theory of probable cause occurs early when diagnosing the issue. Establishing a plan of action comes before implementing changes. Implementing the solution happens during remediation. However, none of these involve summarizing and communicating results after the fact.

Therefore, updating leadership on results corresponds directly to the documentation and lessons-learned phase of the troubleshooting methodology.

NEW QUESTION: 223

Which of the following could provide a lightweight and private connection to a remote box?

- A. Site-to-site VPN
- B. Telnet
- C. Console
- D. Secure Shell

Answer: ([SHOW ANSWER](#))

Secure Shell (SSH) is a protocol used to securely access remote devices over an unsecured network. It provides encrypted command-line access and is a lightweight and secure method of remote administration.

- * A. Site-to-site VPN connects entire networks, not just a single host.
- * B. Telnet is not secure; it transmits data (including credentials) in plaintext.

* C. Console access is direct via serial cable, not remote.

#Reference:

CompTIA Network+ N10-009 Official Objectives: 2.6 - Configure and troubleshoot remote access.

NEW QUESTION: 224

New access points need to be added to the network to increase Wi-Fi coverage. However, no Ethernet connections are available. Which of the following will accomplish this task?

- A. Enabling PoE
- B. Band steering
- C. Mesh deployment
- D. Directional antennas

Answer: ([SHOW ANSWER](#))

A mesh deployment is the correct solution when additional access points are needed but Ethernet connections are not available. In a wireless mesh network, access points can connect to each other wirelessly instead of each AP requiring a direct wired Ethernet uplink. This allows organizations to extend wireless coverage into areas where running new cabling is difficult, expensive, or unavailable. Mesh APs typically use a wireless backhaul connection to forward client traffic toward a wired AP or gateway.

The CompTIA Network+ N10-009 objectives include wireless network design, access point deployment models, coverage expansion, and infrastructure considerations. Mesh networking is especially useful for warehouses, campuses, outdoor spaces, temporary deployments, older buildings, or areas where cabling limitations exist.

Enabling PoE would help power an AP through Ethernet, but the scenario states that no Ethernet connections are available. Band steering encourages capable clients to use a preferred frequency band, usually 5 GHz or 6 GHz, but it does not add AP connectivity. Directional antennas can focus signal coverage in a specific direction, but they do not solve the absence of wired uplinks for new APs. Therefore, mesh deployment is the best answer.

NEW QUESTION: 225

A network engineer is testing a website to ensure it is compatible with IPv6. After attempting to ping the website by its IPv6 address, the engineer determines that the DNS has not been set up properly. Which of the following should the network engineer complete to resolve this issue?

- A. Enable a PTR record.
- B. Update the existing TXT record.
- C. Add a new AAAA record.
- D. Configure a secondary NS record.

Answer: ([SHOW ANSWER](#))

*AAAA records map domain names to IPv6 addresses, enabling proper resolution.

*PTR records (A) are for reverse DNS lookups.

*TXT records (B) store text-based information, not IP addresses.

*NS records (D) define authoritative name servers but don't directly affect IPv6 resolution.

#Reference: CompTIA Network+ N10-009 Official Documentation - DNS Configuration & IPv6.

NEW QUESTION: 226

A network manager connects two switches together and uses two connecting links. Which of the following configurations will prevent Layer 2 loops?

- A. 802.1Q tagging
- B. Full duplex
- C. Link aggregation
- D. QoS

Answer: ([SHOW ANSWER](#))

Link aggregation (also known as port trunking or EtherChannel) combines multiple network connections in parallel to increase throughput and provide redundancy. When two switches are connected with multiple links without any additional configuration, a Layer 2 loop may occur. Link aggregation prevents these loops by treating the multiple connections as a single logical link, using a protocol such as LACP (Link Aggregation Control Protocol).

From Andrew Ramdayal's guide:

"Link aggregation allows you to combine multiple network connections to increase the bandwidth and provide redundancy. It helps prevent Layer 2 loops when connecting switches with multiple links by making them operate as a single logical interface."

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here: <https://www.edudump.com/exams/CompTIA/N10-009/premium/> (**608** Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 227

A company is migrating a data center from on premises to the cloud. Which of the following tools will help maintain consistency, reliability, and efficiency of provisioning and management?

- A. IaC
- B. CDN
- C. SASE
- D. ZTA

Answer: A ([LEAVE A REPLY](#))

The correct answer is A. IaC . Infrastructure as Code is used to define and deploy infrastructure through templates, configuration files, or code rather than building everything manually. During a cloud migration, that approach helps keep deployments consistent across environments and reduces the chance of human error.

This fits the question especially well because it mentions consistency, reliability, and efficiency in both provisioning and management. Those are exactly the kinds of benefits IaC is meant to provide. Instead of configuring servers, networks, and services one by one, administrators can reuse tested deployment definitions and apply the same settings repeatedly. That makes rollouts faster and easier to audit.

The other options do not match the task. A CDN improves content delivery performance. SASE is a networking and security architecture. ZTA focuses on access control and trust decisions. All of those are important in the right context, but none is primarily a provisioning and management automation tool.

In a cloud migration, the organization usually wants repeatable builds, standardization, and faster recovery if something has to be recreated. That is why IaC is the strongest answer here. It directly supports automated, dependable, and scalable infrastructure deployment.

NEW QUESTION: 228

A network administrator upgrades the network infrastructure from copper wiring to fiber connections to increase throughput between network closets. After the upgrade, most of the new connections come online, but one connection remains offline. During troubleshooting with a visual fault locator, the administrator verifies that the final connection was terminated properly. Which of the following is the most likely issue with the fiber connection?

- A. Transposed TX/RX
- B. Incorrect SFP
- C. Incompatible cable
- D. CRC errors

Answer: ([SHOW ANSWER](#))

The most likely issue is transposed TX/RX. Fiber connections require the transmit strand on one side to connect to the receive strand on the other side, and vice versa. If transmit is connected to transmit and receive is connected to receive, the physical termination may be correct, but the link will not come online because the devices cannot properly send and receive optical signals.

The CompTIA Network+ N10-009 objectives include fiber media, transceivers, connectors, cabling issues, and troubleshooting physical connectivity. A visual fault locator can confirm continuity and help identify breaks, bends, or termination problems, but it does not always prove that the transmit and receive strands are correctly crossed between endpoints.

An incorrect SFP could also cause a fiber link failure, but the question emphasizes that only one connection remains offline after most links came online and that the termination was verified. That makes a polarity issue, such as reversed transmit and receive strands, the strongest answer. Incompatible cable is less likely if similar connections are working. CRC errors usually indicate a link is active but experiencing frame errors, not completely offline. Therefore, transposed TX/RX is correct.

NEW QUESTION: 229

An administrator wants to find the top destination for traffic across the infrastructure on a specific day. Which of the following should the administrator use?

- A. SNMP
- B. Packet capture
- C. NetFlow
- D. traceroute

Answer: ([SHOW ANSWER](#))

NetFlow (and similar flow technologies like IPFIX/sFlow in concept) is used to collect traffic-flow metadata such as source/destination IPs, ports, protocols, interfaces, and byte/packet counts over time. In Network+ (N10-009) operations and monitoring objectives, flow data is ideal for identifying top talkers and top destinations across the network on a given day because it provides summarized, queryable information at scale without capturing every packet payload. An administrator can review reports to determine which destination IPs/hosts consumed the most bandwidth, which applications were most active, and what time ranges saw spikes-perfect for historical analysis.

SNMP is great for polling device counters (interface utilization, errors, CPU) but it does not natively tell you the "top destination" by conversation/flow without additional flow awareness. Packet capture can reveal exact conversations and payloads, but it is heavy, localized, and not efficient for infrastructure-wide daily top- destination reporting. traceroute maps the path to a destination and helps isolate routing/path issues; it does not provide usage statistics. Therefore, NetFlow is the best fit.

NEW QUESTION: 230

A company is purchasing a 40Gbps broadband connection service from an ISP. Which of the following should most likely be configured on the 10G switch to take advantage of the new service?

- A. 802.1Q tagging
- B. Jumbo frames
- C. Half duplex
- D. Link aggregation

Answer: ([SHOW ANSWER](#))

Since the switch supports only 10Gbps per port, achieving 40Gbps throughput requires link aggregation (LACP), which combines multiple 10Gbps links into one logical interface for higher bandwidth.

Breakdown of Options:

- A). 802.1Q tagging - VLAN tagging helps segment traffic but does not increase throughput.
- B). Jumbo frames - Jumbo frames reduce overhead but do not increase bandwidth.
- C). Half duplex - Half duplex restricts communication, reducing performance instead of improving it.
- D). Link aggregation - Correct answer. LACP combines multiple 10Gbps links to provide a 40Gbps connection.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 1.2: Compare and contrast network topologies and technologies.

IEEE 802.3ad: Link Aggregation Control Protocol (LACP)

NEW QUESTION: 231

A network administrator recently configured an autonomous wireless AP and performed a throughput test via [comptiaspeedtester.com](#). The result was 75 Mbps. When connected to other APs, the results reached 500 Mbps. Which of the following is most likely the reason for this difference?

- A. Channel width configuration
- B. DNS server issues
- C. Authentication failure
- D. Incorrect DHCP settings

Answer: ([SHOW ANSWER](#))

The channel width (20 MHz vs. 40 MHz vs. 80 MHz) directly impacts Wi-Fi throughput. If the AP is configured with a narrow channel width (e.g., 20 MHz), maximum data rates will be significantly lower than other APs using wider channels (e.g., 80 MHz). This matches the scenario where one AP achieves only ~75 Mbps, while others reach 500 Mbps.

- * B. DNS issues affect name resolution, not raw throughput.
- * C. Authentication failure would prevent connection, not reduce throughput.
- * D. DHCP issues would prevent obtaining an IP, not cause slower speeds.

References (CompTIA Network+ N10-009):

- * Domain: Network Troubleshooting - Wireless throughput issues, channel width configuration.

NEW QUESTION: 232

An imaging workstation at a hospital is experiencing intermittent connectivity loss. Which of the following would most likely be used to resolve the issue at the least expense?

- A. Single-mode fiber
- B. Twinaxial cable
- C. Spanning tree
- D. Shielded twisted pair

Answer: ([SHOW ANSWER](#))

The correct answer is Shielded Twisted Pair (STP). According to the CompTIA Network+ N10-009 objectives, intermittent connectivity issues-especially in environments like hospitals-are often caused by electromagnetic interference (EMI) from medical imaging equipment, power systems, and other electronic devices. These environments are electrically noisy and can disrupt standard copper Ethernet cabling. STP cabling is specifically designed to mitigate EMI by incorporating shielding around the twisted pairs. This shielding reduces external interference and improves signal stability without requiring a complete redesign of the network. Importantly, STP is significantly less expensive than deploying fiber-optic solutions while still being highly effective in environments prone to interference. Single-mode fiber would eliminate EMI entirely, but it is far more costly due to specialized cabling, transceivers, and installation requirements. Twinaxial cable is typically used for short-distance, high-speed data center connections and is not appropriate for workstation connectivity. Spanning Tree Protocol (STP) is a Layer 2 loop-prevention protocol and has nothing to do with physical connectivity or interference issues. The Network+ objectives stress choosing solutions that balance effectiveness, cost, and environmental suitability. In this case, upgrading to shielded twisted pair cabling provides the most practical and cost-effective resolution for intermittent connectivity in a hospital imaging environment.

NEW QUESTION: 233

Which of the following should a network technician do to maintain remote administrative redundancy if a switch becomes unresponsive through SSH?

- A.** Deploy a jump host
- B.** Use an out-of-band management solution
- C.** Enable an administrative GUI
- D.** Connect a physical console cable

Answer: (SHOW ANSWER)

An out-of-band management solution is the best answer because it provides an alternate administrative path to network equipment when the normal production network path is unavailable. If a switch becomes unresponsive through SSH, the technician needs a separate management method that does not depend on the same in-band network connectivity. Out-of-band management can use a dedicated management network, console server, cellular connection, modem, or management interface to reach devices during outages or configuration failures.

The CompTIA Network+ N10-009 objectives include network operations, device management, availability, and remote access methods. SSH is an in-band management method when accessed over the production network. If routing, VLANs, ACLs, management services, or switch control-plane functions are affected, SSH may fail. Out-of-band access improves administrative redundancy and supports recovery.

A jump host can centralize administrative access, but it still depends on network connectivity to the switch.

An administrative GUI may also fail if management access is unavailable. A physical console cable can work locally, but the question specifically asks for remote administrative redundancy. Therefore, an out-of-band management solution is the best answer.

NEW QUESTION: 234

Which of the following concepts describes the idea of housing different customers in the same public cloud data center?

- A.** Elasticity
- B.** Hybrid cloud
- C.** Scalability
- D.** Multitenancy

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation (aligned to N10-009):

Multitenancy is a cloud concept where multiple customers share the same physical resources (servers, storage, and networks) but remain logically separated for security and privacy.

- A). Elasticity is auto-scaling resources.
- B). Hybrid cloud combines private and public resources.
- C). Scalability is the ability to grow resources but doesn't imply multiple customers.

References (CompTIA Network+ N10-009):

Domain: Networking Concepts - Cloud computing models, multitenancy in public cloud.

NEW QUESTION: 235

Which of the following physical installation factors is the most important when a network switch is installed in a sealed enclosure?

- A.** Fire suppression
- B.** Power budget
- C.** Temperature
- D.** Humidity

Answer: ([**SHOW ANSWER**](#)**)**

Switches in sealed enclosures are at risk of overheating because airflow is restricted. The temperature factor is critical since heat buildup can damage components, shorten device lifespan, and cause outages. Proper cooling or ventilation must be ensured.

- A). Fire suppression is important for data centers but not the primary concern in a sealed box.
- B). Power budget applies to PoE allocations, not environmental safety.
- D). Humidity matters, but overheating is far more immediate in sealed environments.

References (CompTIA Network+ N10-009):

Domain: Network Infrastructure - Environmental considerations, switch installation, temperature control.

NEW QUESTION: 236

A network engineer configures the network settings in a new server as follows:

IP address = 192.163.1.15

Subnet mask = 255.255.255.0

Gateway = 192.163.1.255

The server can reach other hosts on the same subnet successfully, but it cannot reach hosts on different subnets. Which of the following is most likely configured incorrectly?

- A.** Subnet mask
- B.** Gateway
- C.** Default route
- D.** IP address

Answer: ([**SHOW ANSWER**](#)**)**

The default gateway for a network should be an IP address within the subnet, but not the broadcast address. In this case:

IP: 192.163.1.15

Subnet Mask: 255.255.255.0

This means the network range is: 192.163.1.0 - 192.163.1.255

192.163.1.255 is the broadcast address for this subnet, so it cannot be used as a gateway.

Hence, the device fails to communicate outside its subnet because it's trying to use a broadcast address as its gateway.

The issue is clearly with the gateway configuration.

Reference:CompTIA Network+ N10-009 Official Study Guide - Objective 1.4: "Given a scenario, configure and deploy common Ethernet switching features."

NEW QUESTION: 237

Which of the following technologies is the best choice to listen for requests and distribute user traffic across web servers?

- A.** Router
- B.** Switch
- C.** Firewall
- D.** Load balancer

Answer: D ([LEAVE A REPLY](#))

A load balancer is designed to distribute user requests across multiple servers to ensure high availability and performance.

Breakdown of Options:

- A). Router - Directs traffic between networks, not between web servers.
- B). Switch - Works at Layer 2, does not distribute web traffic.
- C). Firewall - Secures network traffic, but does not distribute load.
- D). Load balancer - # Correct answer. Optimizes web traffic distribution across multiple servers.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 1.5: Explain load balancing and redundancy concepts.

NEW QUESTION: 238

A network administrator needs to connect a multimode fiber cable from the MDF to the server room. The administrator connects the cable to Switch 2, but there is no link light. The administrator tests the fiber and finds it does not have any issues. Swapping the connection to Switch 1 in a working port is successful, but the swapped connection does not work on Switch 2. Which of the following should the administrator verify next?

- A.** Fiber length
- B.** Transceiver model
- C.** Connector type
- D.** Port speed

Answer: ([SHOW ANSWER](#)**)**

The most probable issue is with the transceiver model. Not all transceivers are compatible with multimode fiber, and the specific type (e.g., SFP, SFP+) and its wavelength must match the fiber cable type. If a port works on one switch but not the other with the same cable, this is a strong indicator of incompatible or faulty transceiver hardware.

Reference:Section 1.5 - Transmission Media and Transceivers - "Transceivers and Compatibility"

NEW QUESTION: 239

Which of the following protocols is used to route traffic on the public internet?

- A.** BGP
- B.** OSPF
- C.** EIGRP
- D.** RIP

Answer: ([SHOW ANSWER](#)**)**

Border Gateway Protocol (BGP) is the primary protocol used to route traffic on the public internet. It allows ISPs and large networks to exchange routing information, making it an Exterior Gateway Protocol (EGP).

Breakdown of Options:

- A). BGP - Correct answer. Used for internet routing and exchanges routing information between ISPs.
- B). OSPF - An Interior Gateway Protocol (IGP) used for routing within an autonomous system (not the public internet).
- C). EIGRP - Cisco's proprietary IGP, used within private networks, not the public internet.
- D). RIP - An older distance-vector protocol, not scalable for the internet.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 1.4: Explain routing technologies.

RFC 4271: Border Gateway Protocol 4 (BGP-4)

NEW QUESTION: 240

Early in the morning, an administrator installs a new DHCP server. In the afternoon, some users report they are experiencing network outages. Which of the following is the most likely issue?

- A. The administrator did not provision enough IP addresses.
- B. The administrator configured an incorrect default gateway.
- C. The administrator did not provision enough routes.
- D. The administrator did not provision enough MAC addresses.

Answer: (SHOW ANSWER)

When a DHCP server is installed and not enough IP addresses are provisioned, users may start experiencing network outages once the available IP addresses are exhausted. DHCP servers assign IP addresses to devices on the network, and if the pool of addresses is too small, new devices or those renewing their lease may fail to obtain an IP address, resulting in network connectivity issues. References: CompTIA Network+ study materials.

NEW QUESTION: 241

A company implements a video streaming solution that will play on all computers that have joined a particular group, but router ACLs are blocking the traffic. Which of the following is the most appropriate IP address that will be allowed in the ACL?

- A. 127.0.0.1
- B. 172.17.1.1
- C. 224.0.0.1
- D. 240.0.0.1

Answer: (SHOW ANSWER)

224.0.0.1 is a multicast address that allows packets to be sent to all hosts within a multicast group. Since video streaming often uses multicast to efficiently distribute data to multiple clients without unnecessary duplication, this is the correct answer.

*Why not the other options?

*127.0.0.1 (A) - This is the loopback address used for internal device testing, not for multicast traffic.

*172.17.1.1 (B) - This is a private unicast address, meaning it can only send packets to one specific host.

*240.0.0.1 (D) - This falls within the reserved experimental IP address range and is not used for multicast.

Reference:

CompTIA Network+ (N10-009) Official Guide - Chapter 7: IP Addressing and Subnetting

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here: <https://www.edudump.com/exams/CompTIA/N10-009/premium/> (**608** Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 242

A network administrator is planning to host a company application in the cloud, making the application available for all internal and third-party users. Which of the following concepts describes this arrangement?

- A. Multitenancy
- B. VPC
- C. NFV
- D. SaaS

Answer: ([SHOW ANSWER](#))

Multitenancy is a cloud computing architecture where a single instance of software serves multiple customers or tenants. Each tenant's data is isolated and remains invisible to other tenants. Hosting a company application in the cloud to be available for both internal and third-party users fits this concept, as it allows shared resources and infrastructure while maintaining data separation and security. References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 243

A network administrator performed upgrades on a server and installed a new NIC to improve performance. Following the upgrades, users are unable to reach the server. Which of the following is the most likely reason.

- A. The PoE power budget was exceeded.
- B. TX/RX was transposed.
- C. A port security violation occurred.
- D. An incorrect cable type was installed.

Answer: ([SHOW ANSWER](#))

When a network administrator installs a new Network Interface Card (NIC) and users are unable to reach the server, one of the common issues is the use of an incorrect cable type. Network cables must match the specifications required by the NIC and the network infrastructure (e.g., Cat5e, Cat6 for Ethernet).

* NIC Compatibility: The new NIC might require a specific type of cable to function properly. Using a cable not rated for the NIC's required speeds or capabilities can result in connectivity issues.

* Cable Standards: Different NICs and network devices might need different cabling standards (straight-through vs. crossover cables, or specific fiber optic types).

* Connection Types: Ensuring that the cable connectors are appropriate for the NIC ports (e.g., RJ45 for Ethernet, LC connectors for fiber optics).

Network References:

* CompTIA Network+ N10-007 Official Certification Guide: Discusses network cabling standards and NIC specifications.

* Cisco Networking Academy: Provides insights into cabling and NIC configurations for optimal network performance.

* Network+ Certification All-in-One Exam Guide: Offers comprehensive details on troubleshooting network connectivity issues, including cabling problems.

NEW QUESTION: 244

Which of the following is the next step to take after successfully testing a root cause theory?

- A. Determine resolution steps.
- B. Duplicate the problem in a lab.
- C. Present the theory for approval.
- D. Implement the solution to the problem.

Answer: (SHOW ANSWER)

* Troubleshooting Methodology:

* Confirming the Root Cause: After testing and confirming the theory, the next logical step is to address the issue by implementing a solution.

* Implementation of the Solution:

* Resolve the Issue: Implement the identified solution to rectify the problem. This step involves making necessary changes to the network configuration, replacing faulty hardware, or applying software patches.

* Documentation: Document the solution and the steps taken to resolve the issue to provide a reference for future troubleshooting.

* Comparison with Other Steps:

* Determine Resolution Steps: This is part of the implementation process where specific actions are outlined, but the actual next step after testing is to implement those steps.

* Duplicate the Problem in a Lab: This step is typically done earlier in the troubleshooting process to understand the problem, not after confirming the root cause.

* Present the Theory for Approval: In some scenarios, presenting the theory might be necessary for major changes, but generally, once the root cause is confirmed, the solution should be implemented.

* Final Verification:

* After implementing the solution, it is important to verify that the issue is resolved and that normal operations are restored. This may involve monitoring the network and testing to ensure no further issues arise.

References:

* CompTIA Network+ study materials on troubleshooting methodologies and best practices.

NEW QUESTION: 245

Which of the following is used to redistribute traffic between one source and multiple servers that run the same service?

- A. Router
- B. Switch
- C. Firewall
- D. Load balancer

Answer: (SHOW ANSWER)

The correct answer is Load balancer because it is specifically designed to distribute incoming network traffic across multiple backend servers that provide the same application or service. According to CompTIA Network+ (N10-009) objectives under network infrastructure, load balancing improves performance, scalability, and high availability by preventing any single server from becoming overwhelmed.

A load balancer can operate at Layer 4 (transport layer, based on IP address and port) or Layer 7 (application layer, based on content such as HTTP headers or URLs). It uses various algorithms such as round-robin, least connections, or weighted distribution to efficiently allocate client requests among servers. If one server fails, the load balancer can redirect traffic to healthy servers, ensuring service continuity.

A router (Option A) forwards packets between different networks but does not distribute traffic among servers running the same application. A switch (Option B) forwards frames within a local network based on MAC addresses. A firewall (Option C) filters traffic based on security rules but does not perform traffic distribution for load-sharing purposes.

Therefore, a load balancer is the correct solution for redistributing traffic among multiple servers.

NEW QUESTION: 246

Which of the following is an XML-based security concept that works by passing sensitive information about users, such as login information and attributes, to providers?

- A.** IAM
- B.** MFA
- C.** RADIUS
- D.** SAML

Answer: ([SHOW ANSWER](#))

The correct answer is SAML (Security Assertion Markup Language). SAML is an XML-based standard used for single sign-on (SSO) and identity federation. It allows identity providers (IdPs) to share authentication and authorization data with service providers (SPs), passing secure tokens containing user attributes and credentials.

A). IAM (Identity and Access Management) is the broader framework, not specifically XML-based.

B). MFA enforces multiple factors for authentication but does not involve XML assertions.

C). RADIUS is an AAA protocol, but it uses UDP, not XML assertions.

SAML is widely used in federated identity systems, enabling secure authentication across different domains and applications without requiring multiple credentials.

References (CompTIA Network+ N10-009):

Domain: Network Security - Authentication methods, SAML, SSO.

NEW QUESTION: 247

Following a fire in a data center, the cabling was replaced. Soon after, an administrator notices network issues. Which of the following are the most likely causes of the network issues? (Select two).

- A.** The switches are not the correct voltage.
- B.** The HVAC system was not verified as fully functional after the fire.
- C.** The VLAN database was not deleted before the equipment was brought back online.
- D.** The RJ45 cables were replaced with unshielded cables.
- E.** The wrong transceiver type was used for the new termination.
- F.** The new RJ45 cables are a higher category than the old ones.

Answer: ([SHOW ANSWER](#))

* Unshielded cables (D) are more prone to interference and may not be suitable for certain environments, especially after a fire where interference could be heightened.

* Using the wrong transceiver (E) for new terminations can lead to compatibility issues, causing network failures.

NEW QUESTION: 248

Which of the following best describes a characteristic of a DNS poisoning attack?

- A.** DNS address records are edited and changed on a DNS server.

- B. An attacker sets up a malicious DNS server in place of a legitimate server.
- C. DNS client requests are intercepted and false responses are returned.
- D. False DNS records are injected into cache on a DNS server.

Answer: ([SHOW ANSWER](#))

DNS poisoning (also commonly called DNS cache poisoning) is characterized by inserting fraudulent DNS data into a resolver's cache so that subsequent queries return incorrect IP mappings. Option D describes this precisely: false DNS records are injected into a DNS server's cache, causing users to be redirected to attacker-controlled destinations even when they request a legitimate hostname. This aligns with Network+ security objectives covering common network attacks targeting name resolution and trust relationships. Editing authoritative DNS records on a DNS server (A) implies direct compromise or unauthorized administrative change, which is a different scenario than cache poisoning. Setting up a malicious DNS server in place of a legitimate server (B) is closer to DNS hijacking or rogue DNS configuration rather than cache poisoning. Intercepting client requests and returning false responses (C) describes man-in-the-middle style spoofing on the wire; while related, the defining "poisoning" trait is the persistence created by corrupting the cache so the bad answer continues to be served. For defensive relevance in Network+ scope, cache poisoning highlights the importance of DNS security controls such as source port randomization, transaction ID entropy, and DNSSEC validation where applicable.

NEW QUESTION: 249

A company is implementing a new wireless network in its office building and wants to ensure maximum coverage and signal strength. Which of the following factors should a technician consider to meet these requirements? Select two.

- A. Building materials
- B. Electrical interference
- C. Distance from the server room
- D. Type of encryption being used
- E. Power over Ethernet
- F. Type of client devices

Answer: ([SHOW ANSWER](#))

Building materials and electrical interference are the two best factors to consider when designing a wireless network for maximum coverage and signal strength. Wireless signals can be weakened or blocked by concrete, brick, metal, glass, insulation, elevator shafts, walls, and other structural materials. These materials can absorb, reflect, or scatter radio frequency signals, creating weak coverage areas or dead zones. Electrical interference is also important because wireless networks can be affected by devices that generate electromagnetic or radio frequency interference. Examples include microwaves, motors, fluorescent lighting, cordless devices, industrial equipment, and neighboring wireless networks. Interference can reduce signal quality, increase retransmissions, and cause unstable connectivity.

The CompTIA Network+ N10-009 objectives include wireless site surveys, signal strength, antenna placement, interference, and environmental factors. These considerations are central to proper wireless design.

Distance from the server room does not directly determine wireless signal coverage. Encryption affects security, not radio signal strength. Power over Ethernet affects how APs receive power but not coverage by itself. Client device type can affect performance, but the best design factors for coverage and signal strength are building materials and electrical interference.

NEW QUESTION: 250

A network engineer is setting up a new VoIP network for a customer. The current network is segmented only for computers and servers. No additional switch ports can be used in the new network. Which of the following does the engineer need to do to configure the network correctly? (Select TWO).

- A. Change network translation definitions
- B. Enable 802.1Q
- C. Implement a routing protocol
- D. Set up voice VLANs
- E. Reconfigure the DNS
- F. Place devices in the perimeter network

Answer: (SHOW ANSWER)

To support VoIP on the same physical ports used by computers:

B). Enable 802.1Q: This standard supports VLAN tagging, allowing voice and data traffic to share the same port using separate VLANs.

D). Set up voice VLANs: Separating voice traffic into its own VLAN improves QoS and manageability.

Other options are not directly related to configuring VoIP over existing ports:

A). Network translation definitions (NAT) are unrelated to switch-level VLAN configuration.

C). Routing protocols are not necessary at the switch level for VLAN setup.

E). DNS is not required for the switch or VLAN setup.

F). Perimeter network (DMZ) is used for public-facing servers, not VoIP VLANs.

Reference:

CompTIA Network+ N10-009 Official Objectives: 2.3 - Given a scenario, configure and verify VLANs.

CompTIA Network+ N10-009 Official Objectives: 3.6 - Explain the characteristics of network topologies and types.

NEW QUESTION: 251

As part of an attack, a threat actor purposefully overflows the content-addressable memory (CAM) table on a switch. Which of the following types of attacks is this scenario an example of?

- A. ARP spoofing
- B. Evil twin
- C. MAC flooding
- D. DNS poisoning

Answer: (SHOW ANSWER)

* Definition of MAC Flooding:

* MAC flooding is an attack where a malicious actor sends numerous fake MAC addresses to a switch, overwhelming its CAM table. The CAM table stores MAC addresses and their associated ports for efficient traffic forwarding.

* Impact of MAC Flooding:

* CAM Table Overflow: When the CAM table is full, the switch cannot learn new MAC addresses and is forced to broadcast traffic to all ports, leading to a degraded network performance and potential data interception.

* Switch Behavior: The switch operates in a fail-open mode, treating the network as a hub, which can be exploited for eavesdropping on traffic.

* Comparison with Other Attacks:

* ARP Spoofing: Involves sending false ARP (Address Resolution Protocol) messages to associate the attacker's MAC address with the IP address of another device.

* Evil Twin: Involves creating a rogue wireless access point that mimics a legitimate one to intercept data.

* DNS Poisoning: Involves corrupting the DNS cache with false information to redirect traffic to malicious sites.

* Preventive Measures:

* Port Security: Configure port security on switches to limit the number of MAC addresses per port, preventing CAM table overflow.

* Network Segmentation: Use VLANs to segment network traffic and limit the impact of such attacks.

References:

* CompTIA Network+ study materials on network security threats and mitigation techniques.

NEW QUESTION: 252

A network administrator must implement a feature that supports redundancy and scaling on the switches at the distribution layer of the network. Which of the following is the best option?

- A.** VLAN assignment
- B.** Spanning tree
- C.** Port speed
- D.** Full duplex

Answer: ([SHOW ANSWER](#))

The correct answer is B. Spanning tree. At the distribution layer, switch redundancy is common because multiple paths are usually built into the design to avoid a single point of failure. The problem with redundant Layer 2 paths is that they can create switching loops, broadcast storms, and unstable MAC address tables if nothing controls them. Spanning Tree Protocol solves that problem by logically blocking one or more redundant paths while still keeping those paths available as backups.

That makes spanning tree the best fit for a feature that supports both redundancy and safe scaling. As the switched environment grows, STP helps maintain a stable topology and prevents loop-related failures. If the active path fails, a blocked redundant path can be brought into service. The other options do not address the real need. VLAN assignment is used to segment broadcast domains, but it does not manage redundant Layer 2 paths. Port speed only affects throughput on an interface. Full duplex improves communication efficiency on a link, but it also does not provide redundancy control or loop prevention.

When a Network+ question mentions redundancy on switches and asks for the best switching feature, spanning tree is the strongest answer.

NEW QUESTION: 253

Which of the following should an installer orient a port-side exhaust to when installing equipment?

- A.** The patch panel
- B.** The front of the IDF
- C.** The warm aisle
- D.** The administrator console

Answer: ([SHOW ANSWER](#))

In data centers, hot aisle/cold aisle configurations are used to manage airflow and cooling efficiency. Port-side exhausts should be oriented towards the warm aisle to expel hot air and maintain optimal cooling. The document clarifies:

"Equipment with port-side exhausts should be oriented towards the warm aisle to ensure that hot air is properly directed away from the cold air intake areas. This alignment supports effective cooling in data center environments."

NEW QUESTION: 254

A technician is planning an equipment installation into a rack in a data center that practices hot aisle/cold aisle ventilation. Which of the following directions should the equipment exhaust face when installed in the rack?

- A.** Sides
- B.** Top
- C.** Front

D. Rear

Answer: ([SHOW ANSWER](#))

In a data center that uses hot aisle/cold aisle ventilation, equipment is typically installed so that cool air enters from the cold aisle (front) and hot air is exhausted to the hot aisle (rear). This configuration maximizes cooling efficiency.

NEW QUESTION: 255

Which of the following is the best VPN to use for reducing data bandwidth requirements of the corporate network?

- A. Split-tunnel
- B. Site-to-site
- C. Full-tunnel client
- D. GRE tunnel

Answer: ([SHOW ANSWER](#))

A split-tunnel VPN allows a device to route some traffic through the VPN (typically corporate traffic) while sending other traffic (like general internet browsing) directly over the local internet connection. This reduces the load on the corporate network because not all traffic is routed through the VPN tunnel.

Site-to-site VPNs are for permanent links between locations.

Full-tunnel VPNs route all traffic through the VPN, increasing the bandwidth usage on the corporate network.

GRE (Generic Routing Encapsulation) is a tunneling protocol that doesn't encrypt and doesn't reduce bandwidth usage by itself.

Reference:

CompTIA Network+ N10-009 Official Objectives: 3.3 - Given a scenario, configure and deploy common VPN technologies.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here: <https://www.edudump.com/exams/CompTIA/N10-009/premium/> (608 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)